JPA 6-282527

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06282527 A**

(43) Date of publication of application: **07.10.94**

(51) Int. Cl **G06F 15/00**
G06F 15/00
G06F 13/00
G06F 15/16
H04L 12/24
H04L 12/26
H04M 3/42

(21) Application number: **05069751**

(22) Date of filing: **29.03.93**

(71) Applicant: **HITACHI SOFTWARE ENG CO LTD**

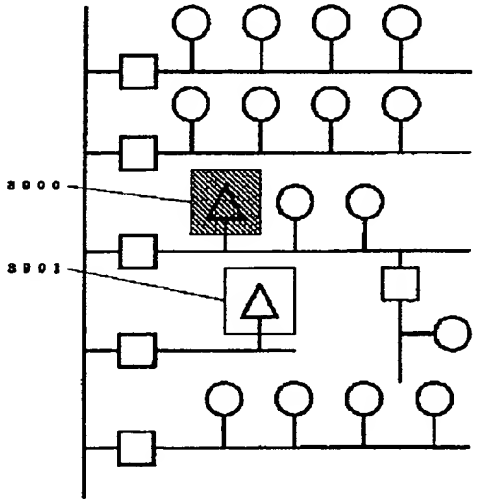
(72) Inventor: **KONDOU MARIKO**
MORI YUMIKO
TSUTSUMI TOSHIYUKI

(54) **NETWORK CONTROL SYSTEM**

(57) Abstract:

PURPOSE: To detect a security hole on a network and to take measures for it.

CONSTITUTION: A security hole is detected in a network and the security hole is displayed on the constitution drawing of the network. Further, the display of the connection status from an external network, the access contents for an electronic computer and a network equipment, the access status to a setting file for maintaning network environments and the log-in status in a privileged user are displayed on the constitution drawing. The display is performed so that the difference may be recognized by the method how an electronic computer where all the monitoring programs are working is displayed by oblique lines like a code 3900 and an electronic computer having the montiroing programs which are not working is displayed by only a frame like a code 3901 or the method how colors are changed or display luminance is changed, etc., for instance.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平6－282527

(43)公開日　平成６年(1994)10月７日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
G06F 15/00	330	A 7459-5L		
	310	R 7459-5L		
13/00	351	Z 7368-5B		
15/16	470	M 9190-5L		
H04L 12/24				

審査請求　未請求　請求項の数10　ＯＬ　（全30頁）　最終頁に続く

(21)出願番号　特願平5－69751

(22)出願日　平成５年(1993)３月29日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　近藤　麻里子
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(72)発明者　森　優美子
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

最終頁に続く

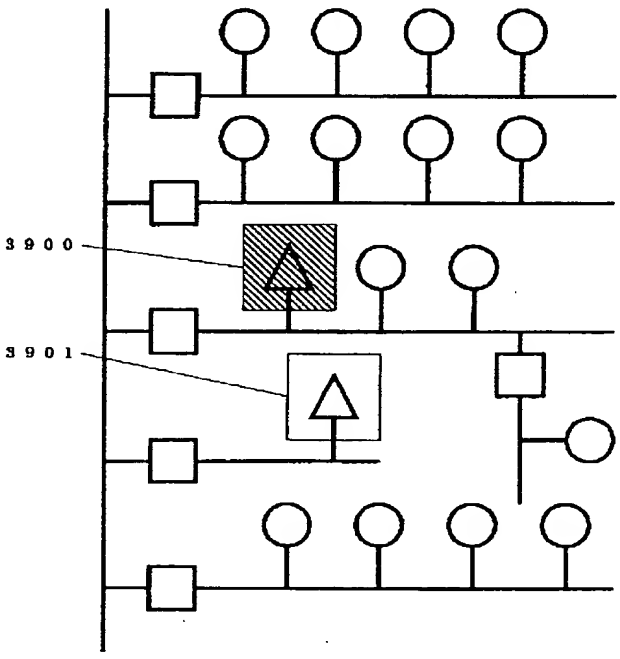
(54)【発明の名称】ネットワーク管理システム

(57)【要約】　(修正有)

【目的】　ネットワーク上でのセキュリティホールを検出し、それに対する対策を講じる。

【構成】　ネットワークにおけるセキュリティホールを検出し、ネットワークの構成図面上に当該セキュリティホールを表示する。さらに、前記構成図面上に外部ネットワークからの接続状況表示、電子計算機及びネットワーク機器に対するアクセス内容、ネットワーク環境維持用設定ファイルへのアクセス状況、特権ユーザでのログイン状況を表示する。例えば、監視プログラムが全て稼働している電子計算機は符号３９００のように斜線で表示し、稼働してない監視プログラムのある電子計算機は符号３９０１のように枠のみで表示するといった方法や、色を変えたり、表示輝度を変えるなどの方法により、違いが判るように表示する。

図３９



1

【特許請求の範囲】

【請求項１】　電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、

前記ネットワーク機器の物理的配置と接続関係に関する情報を格納したデータベースと、ネットワーク構成図等を表示する表示装置と、前記データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を前記表示装置に表示すると共に、前記ネットワークのセキュリティホールを検出し、ネットワークのセキュリティホールの内容や重要度等に応じた表示形態により、前記ネットワーク構成図面上にネットワークのセキュリティホールを表示する手段と、ネットワークのセキュリティホールに対する対策を講じる処理手段とを有するネットワーク－ク管理システム。

【請求項２】　請求項１に記載のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワーク構成図面上の位置への指示操作に対し、前記データベースに格納された物理的ネットワーク構成、論理的ネットワーク構成、ネットワーク配線、フロア図面、地図等の情報を用いて動的かつ論理的な接続状況を表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項３】　請求項１に記載のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワークケーブルへの指示操作に対し、電子計算機、ネットワーク機器及びネットワークケーブルでの通信量を測定し、さらに通信内容の分類と分類別の通信量割合を算出し、その測定結果及び分類結果に基づき通信量の時間的な推移及び変化、全体の通信量に対する分類別の通信量割合を、前記表示装置上に識別可能な形式で表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項４】　請求項１に記載のネットワーク管理システムにおいて、前記ネットワーク構成図に表示された電子計算機及びネットワーク機器への指示操作に対し、前記データベースに格納された物理的ネットワーク構成、論理的ネットワーク構成等の情報を用いて、動的かつ論理的なユーザのログイン状況を検出して表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項５】　請求項１に記載のネットワーク管理システムにおいて、ネットワーク上の電子計算機及びネットワーク機器で定義されたネットワーク環境を保持する環境設定ファイルに対するアクセス履歴を随時、前記データベースに格納する手段と、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、前記環境設定ファイルに対するアクセス履歴から一定期間内のものを抽出し、その抽出結果を前記表示装置上に表示する手段と設けることを特徴とするネットワーク管理システム。

2

【請求項６】　請求項１に記載のネットワーク管理システムにおいて、ネットワーク上の電子計算機及びネットワーク機器で定義された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で現在稼働中であるプログラム及びコマンド群の中から前記条件に合致しないプログラム及びコマンド、合致していても外部からの侵入可能性のあるプログラム及びコマンド、内部での不正使用の可能性あるプログラム及びコマンドを随時、前記データベースに格納する手段と、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、前記データベースに格納したプログラム及びコマンドの動作状況を前記表示装置上に表示する手段とを設けることを特徴とするネットワーク管理システム。

【請求項７】　請求項１のネットワーク管理システムにおいて、論理的または物理的なネットワーク構成図面を前記表示装置に表示させ、ネットワーク上の電子計算機及びネットワーク機器で定義された特権ユーザによるネットワークへのログイン履歴を随時、前記データベースに格納する手段と、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、前記データベースに格納した特権ユーザによるネットワークへのログイン履歴から一定期間内のものを抽出し、その抽出結果を前記表示装置上に表示する手段を設けることを特徴とするネットワーク管理システム。

【請求項８】　請求項１のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、電子計算機及びネットワーク機器で定義されたネットワーク接続用環境設定ファイルの内容を、予め前記データベースに格納されたネットワークへのアクセス許諾条件等の情報に基づき照合及び検査する手段と、その結果を前記表示装置上に表示し、さらに緊急度・重要度に応じて通知を行う手段とを設けることを特徴とするネットワーク管理システム。

【請求項９】　請求項１のネットワーク管理システムにおいて、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等への指示操作に対し、予め前記データベースに格納された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で稼働可能なプログラム及びコマンド群の中から前記条件に合致しないプログラム及びコマンド、合致していても外部からの侵入可能性のあるプログラム及びコマンド、内部での不正使用の可能性があるプログラム及びコマンドがあるかどうかを照合及び検査する手段と、その結果を前記表示装置上に表示する手段とを設けることを特徴とするネットワーク管理システム。

【請求項１０】　請求項１のネットワーク管理システム

において、前記ネットワーク構成図面上で、ネットワーク監視を行っている電子計算機及びネットワーク機器をセキュリティレベルに応じて識別可能な形式で表示する手段を設けることを特徴とするネットワーク管理システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、複数の電子計算機及びネットワーク機器が接続されているコンピュータネットワークに関し、特に、ネットワークを円滑に運用管理するためのネットワーク管理システムに関するものである。

【０００２】

【従来の技術】ネットワークの基盤となる通信技術の発達により、ここ数年の間に高速で信頼性の高いネットワーク構築が可能になったため、年々その規模は大きく、広域化が進んでいる。

【０００３】現在、ネットワーク管理作業の効率化を図るための「ネットワーク管理ツール」と呼ばれるシステムが各社から提案されている。こうしたツールの共通点は、SNMP（Simple Network Management Protcol）やCMIP（Common Management InformationProtocols）等の通信プロトコルを用いたネットワークの管理を行うという点である。

【０００４】プロトコルレベルのネットワーク管理機能とは、ネットワークトラフィックのモニタリング機能、モニタリング結果をまとめる統計処理機能、トラフィック異常時のアラーム発生機能などである。

【０００５】また、ネットワークのセキュリティ管理システムに関しては、

（１）特開昭６２－２１１７６５号公報の「コンピュータシステムの利用者チェック装置」

（２）特開平０１－７６２６１号公報の「情報処理システムの不正侵入判断方式」

（３）特開平０１－１９６６５５号公報の「不正ログイン防止方式」

（４）特開平０１－２２４８５８号公報の「コンピュータの不正アクセス防止方法及びそれに用いるボード装置」

（５）特開平０１－２９３０４０号公報の「回線接続許可装置」

（６）特開平０２－１９２３３９号公報の「ハッカー侵入防止方式」

（７）特開平０３－２５８１５２号公報の「通信サービス方式」

（８）特開平０２－３６４５６号公報の「ハッカー防止装置およびそのキーワード作成方法」

などがある。

【０００６】前記（１）のコンピュータシステムの利用者チェック装置は、端末を使用する利用者にＩＤコードを入力させ、そのＩＤコードを端末側とホスト側の両方で暗号処理装置により２次暗号を生成し、両者の２次暗号を比較し、一致した場合に暗号処理コードを更新することで、容易にコンピュータシステムへの侵入を行えないようにするものである。

【０００７】前記（２）の情報処理システムの不正侵入判断方式は、接続要求を行った端末に対し利用者ＩＤコードを要求し、さらに、その端末に対し信号を送出する。利用者ＩＤコードから求められる予め記憶された信号往復時間と接続要求のあった端末までの信号往復時間とを比較し、所定時間差以外の場合に接続を拒否するものである。

【０００８】前記（３）の不正ログイン防止方式は、不正なログイン試行を検出する手段及び不正ログインに対し疑似動作を行う手段を用い、侵入者の操作を監視し、ログイン時間を長引かせることで、ホストコンピュータへの侵入を防止するものである。

【０００９】前記（４）のコンピュータの不正アクセス防止方法及びそれに用いるボード装置は、コンピュータへのアクセス時に２つ以上のコード入力を促し、全てのコード入力が終了した時点で正誤判定を行い、組合せの数を大きくさせ、不正アクセスを目的としたハッカーのコード検索を困難にさせるものである。

【００１０】前記（５）の回線接続許可装置は、接続可否情報を予め設定し、接続要求メッセージが入力された時点で、この情報に基づき接続可否判定を行うことで、コンピュータ装置への不正アクセスを防止するものである。

【００１１】前記（６）のハッカー侵入防止方式は、電話回線を用いた端末のコンピュータ接続時に、端末から暗証番号を２度入力させ、一定時間内に正しい暗証番号が送信されなければ、回線を切断するものである。

【００１２】前記（７）の通信サービス方式は、公衆回線網を用いたネットワークシステムにおいて、暗号ＩＤ発生機能付電話機から送付される装置ＩＤ及び暗号ＩＤを、予め登録してある加入者側の装置ＩＤ及び暗号ＩＤと比較することで、通信サービス許可の可否判定を行い、特定加入者のみに通信サービスを提供するものである。

【００１３】前記（８）のハッカー防止装置およびそのキーワード作成方法は、端末からホストに送信するデータに、端末ＩＤとパスワード、さらに、端末側で作成するキーワードを付加し、ハッカー防止装置によりキーワードの照合を行い、不一致の場合には回線を切断することで、バグ混入プログラム等の送信を防止するものである。

【００１４】

【発明が解決しようとする課題】しかしながら、前記従来の技術では、以下に挙げるような問題がある。

【００１５】（１）ネットワークのセキュリティホール

の検出と対策

電子計算機及びネットワーク機器をネットワーク接続して使用する場合、どこの端末からでも同様のサービスと使い易い環境を提供することと、外部からの侵入やネットワーク環境の不正使用防止は、相反する場合が多い。言い換えると、ネットワークの構築はセキュリティホールを作り出すことであるとも言える。

【００１６】そこで、前記従来の技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、不当なアドレスを有する接続機器の検出や、ネットワーク上を流れているデータのログ内容から不正なネットワーク利用者の検出を行う機能を有しているものがある。しかし、こうしたシステムでは、ネットワークのどの部分がセキュリティホールとなったかが把握できない。

【００１７】すなわち、ネットワークに関する各種の設定条件等が実際に安全な設定になっているか、或は、使い易さのために部分的にセキュリティチェックを緩和させていないかといったことを、自動的に検出することができない。したがって、セキュリティ確保のための対策を予め講じておくことも困難になる。

【００１８】さらに、前記従来の技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、論理的な接続関係に基づくネットワーク構成図を表示するものが一般的であり、機器の物理的な配置（レイアウト）、例えば、どのビルの何階のどの部署のどの位置で接続しているかを表示できるものはない。

【００１９】（２）外部からの侵入、内部での不正利用の早期発見

ネットワークに対する外部からの侵入及び内部での不正利用を完全に防止することは、現在の技術ではまだ困難である。しかし、その可能性をできるだけ低くするために、前記従来の技術で述べたように、セキュリティ管理を行う各種の方式や装置が考えられている。

【００２０】これらの方式や装置は、端末からのログイン時点、或は、回線接続時点での不正なアクセス防止を目的としている。しかし、これらの方式や装置では、ネットワークに侵入された後の不正利用を発見することはできない。

【００２１】また、前記従来の技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、ネットワークトラフィックのモニタリング機能及びモニタリングのログ内容の統計処理機能を用いて、不当なアドレスを有する接続機器の検出や不正なネットワーク利用者の検出を行えるものもある。

【００２２】しかし、こうしたシステムでは、実際に不正が行われ、管理者が何らかの異常な現象に気付き、ネットワークトラフィックのログ調査を開始するまでは、ネットワーク上のどこで何が行われているかを把握できず、早期発見が困難である。

【００２３】さらに、こうした不正アクセス検出はトラフィックデータの内容に依存した方式で行われているため、ネットワーク利用者単位、利用者の実行権限単位、ネットワーク機器上で稼働しているコマンドやプログラムやプロセス単位、ネットワーク管理で使用するファイル単位、或は、ネットワーク機器単位で、不正アクセスを監視することができない。

【００２４】（３）適正なネットワーク利用環境の構築支援

前記従来の技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、ネットワークの性能管理を行うために、ネットワーク上を流れるデータを収集し、その内容及び種別毎の統計処理を行う機能を有するものが多い。

【００２５】しかし、性能管理を行うだけでは、適正なネットワーク利用環境を構築できない。すなわち、ネットワークに接続されている電子計算機、端末等を含むネットワーク機器をどのような条件や権限で使用できるように設定しているかを把握することができない。

【００２６】（４）安全なネットワーク環境の視覚的な把握

前記従来の技術で述べた通信プロトコルレベルでのネットワーク管理システムでは、ネットワークの論理的な接続関係に基づくネットワーク構成図を表示し、接続しているネットワーク機器が稼働しているかどうかを表示する機能を有するものが多い。

【００２７】しかし、そうしたネットワーク構成図の表示では、どのネットワーク機器でどのようなセキュリティ対策を講じているか、或は、どのネットワーク機器でどのような権限でどのようなコマンドやプログラムやプロセスが稼働しているかを視覚的に把握することができない。

【００２８】本発明の第１の目的は、ネットワーク上でのセキュリティホールを検出し、ネットワーク構成図面上でそれを表示し、そのネットワークのセキュリティホールに対する対策を講じることができるネットワーク管理システムを提供することである。

【００２９】本発明の第２の目的は、通常のネットワーク使用状況を常時監視し、一般のネットワーク利用者のネットワーク利用状況や、特権ユーザ権限でしか行えないシステム関連ファイルへのアクセスや、実行時に特権ユーザ権限を得ることのできる特定プロセスの稼働状況や、特権ユーザ権限でのネットワーク機器に対するアクセスを把握し、アクセスの記録を残すことで、外部からの侵入、内部での不正利用の早期発見を可能にすることができるネットワーク管理システムを提供することである。

【００３０】本発明の第３の目的は、ネットワーク環境における様々なアクセス許諾内容の妥当性をチェックし、妥当でない場合はネットワーク管理者に通知を行い、適正なネットワーク利用環境の構築を支援すること

ができるネットワーク管理システムを提供することである。

【００３１】本発明の第４の目的は、ネットワーク管理システムの管理対象となるネットワークをネットワーク構成図面上で表示することで、安全なネットワーク環境の視覚的な把握を行うことができるネットワーク管理システムを提供することである。

【００３２】

【課題を解決するための手段】前記第１の目的を達成するために、前記ネットワーク機器の物理的配置と接続関係に関する情報を格納したデータベースと、ネットワーク構成図等を表示する表示装置と、前記データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を前記表示装置に表示すると共に、前記ネットワークのセキュリティホールを検出し、ネットワークのセキュリティホールの内容や重要度等に応じた表示形態により、前記ネットワーク構成図面上にネットワークのセキュリティホールを表示する管理手段と、ネットワークのセキュリティホールに対する対策を講じる処理手段とを設けた。

【００３３】また、第２の目的を達成するために、本発明は、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワーク構成図面上の位置への指示操作に対し、前記データベースに格納された物理的ネットワーク構成、論理的ネットワーク構成、ネットワーク配線、フロア図面、地図等の情報を用いて動的かつ論理的な接続状況、即ち、現在、どの電子計算機又はネットワーク機器から、或はどんな外部のネットワークから、誰がどのような接続手段で、前記ネットワークに接続しているか、さらに動的なユーザのログイン状況表示、即ち、現在、どの電子計算機、端末、ネットワーク機器から、誰が、どの電子計算機及びネットワーク機器を使用し、どのような処理を行っているかの表示を行う手段とを設けた。

【００３４】あるいは、前記ネットワーク構成図面に表示された電子計算機、ネットワーク機器及びネットワークケーブル等を指示すると、電子計算機、ネットワーク機器及びネットワークケーブルでのネットワーク通信量を測定し、その測定結果に基づいた通信量の時間的な推移及び変化や、通信内容の分類を行い、分類別の通信量割合を算出し、測定結果及び分類結果に基づき、全体の通信量と全体の通信量に対する分類別の通信量割合を、前記表示装置上に識別可能な形式で表示する手段を設けた。

【００３５】あるいは、ネットワーク上の電子計算機及びネットワーク機器で定義されたネットワーク環境を維持するための環境設定ファイルに対するアクセス履歴を随時、前記データベースに格納しておき、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、前記データベースに格納しているネットワーク環境を維持するための環境設定ファイルに対するアクセス履歴から一定期間内のものを抽出し、その抽出結果、即ち、いつ、誰が、どのような変更・参照・追加を行ったかを前記表示装置上に表示する手段を設けた。

【００３６】あるいは、ネットワーク上の電子計算機及びネットワーク機器で定義された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で、現在、稼働中であるプログラム及びコマンド群の中から、前記条件に合致しないものや合致していても外部からの侵入可能性のあるプログラム及びコマンドや内部での不正使用の可能性あるものを随時、前記データベースに格納しておき、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、前記の条件に合致しないものや合致していても外部からの侵入可能性のあるプログラム及びコマンドや内部での不正使用の可能性あるものの動作状況を、前記表示装置上に表示する手段を設けた。

【００３７】あるいは、ネットワーク上の電子計算機及びネットワーク機器で定義された特権ユーザによるネットワークへのログイン履歴を随時、前記データベースに格納しておき、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、前記データベースに格納している特権ユーザによるネットワークへのログイン履歴から、一定期間内のものを抽出し、その抽出結果、即ち、いつ、誰が、どこから、どの電子計算機及びネットワーク機器に対して、特権ユーザ権限で何を行ったかを前記表示装置上に表示する手段を設けた。

【００３８】また、前記第３の目的を達成するために、前記前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、電子計算機及びネットワーク機器で定義されたネットワーク接続用環境設定ファイルの内容を、予め前記データベースに格納されたネットワークへのアクセス許諾条件等の情報に基づき、外部からの不正な侵入や不正な使用を許す環境になっていないかを、照合及び検査し、その結果を前記表示装置上に表示し、さらに、緊急度・重要度に応じ、ネットワーク管理者に対して通知する手段を設けた。

【００３９】あるいは、前記ネットワーク構成図面に表示された電子計算機及びネットワーク機器等を指示すると、予め前記データベースに格納された、ネットワーク上でセキュリティを確保した上で稼働を許諾する条件等の情報に基づき、指示されたネットワーク上の電子計算機及びネットワーク機器で稼働可能なプログラム及びコマンド群の中から、前記条件に合致しないものや合致していても外部からの侵入可能性のあるプログラム及びコマンドや内部での不正使用の可能性あるものがあるかどうかを、照合及び検査し、その結果、即ち、どの機器

で、どのような危険な稼働可能なプログラム及びコマンド等があるかを前記表示装置上に表示する手段を設けた。

【００４０】また、前記第４の目的を達成するために、物理的なネットワーク構成図面上で、ネットワーク監視を行っている電子計算機及びネットワーク機器を、セキュリティレベルに応じて識別可能な形式で表示する手段を設けた。

【００４１】ここで、ネットワークのセキュリティホールとは、複数のネットワーク機器が接続しているネットワークにおける以下のような事項を指す。

（１）外部ネットワークとの接続(アクセス）ポイント、（２）外部ネットワークに対するアクセス許諾条件(論理的侵入可能性)、（３）ネットワーク上を流れる通信内容の偏り、（４）特定ユーザ、プログラム、コマンド等によるネットワークの占有、（５）ネットワーク内に接続しているネットワーク機器を使用しているユーザが稼働させているプログラム及びコマンド群のセキュリティレベル及びユーザ権限、（６）ネットワーク内に接続している計算機以外のネットワーク機器のアクセス許諾条件、（７）ネットワーク内に接続しているネットワーク機器で定義された特権ユーザ権限での起動が可能なプログラム及びコマンドに対するアクセス許諾条件、（８）ネットワーク内に接続しているネットワーク機器の上記条件設定情報へのアクセス許諾条件、（９）ネットワーク内で稼働中のプログラム及びコマンド群のセキュリティレベル及びユーザ権限、(10) 特権ユーザ権限でのプログラム及びコマンドの起動、(11) 論理的に接続しているが、ネットワーク管理システムの管理対象範囲外の内部ネットワーク。

【００４２】

【作用】前述の手段によれば、ネットワークのセキュリティホールを検出し、その検出したセキュリティホールをネットワーク構成図面上に表示するので、ネットワークにおけるセキュリティを確保することができる。

【００４３】また、ネットワーク及びネットワーク機器に対するアクセス状況を常時監視するので、外部からの侵入、内部での不正利用の発見を速やかに行うことができる。

【００４４】さらに、ネットワーク環境設定用ファイルの内容をアクセス許諾条件に基づき照合及び検査するので、適正なネットワーク利用環境の構築を容易に行うことができる。

【００４５】さらに、ネットワーク管理の対象となっているネットワーク機器をネットワー構成図面上で識別可能な形式で表示させるので、安全なネットワーク環境を視覚的に簡単に把握することができる。

【００４６】

【実施例】以下、本発明の実施例を図面を参照して具体的に説明する。

【００４７】図１は本発明の一実施例にかかるネットワーク管理システムの構成を示す図である。

【００４８】図１において、１００はネットワーク管理システムが管理する被管理機器がケーブル類で接続されたネットワークである。１０１は通信制御装置であり、ネットワーク管理システムとネットワーク１００間の通信を制御する。

【００４９】１０２は中央処理装置であり、データ処理、システム制御及び予めプログラムされた各種処理を行う。１０３は入力装置であり、キーボード、マウス、プリンタなどが用いられる。１０４は出力装置であり、ディスプレイ、プリンタなどが用いられる。１０５は、補助記憶装置であり、光磁気ディスク、メタルテープ、ハードディスクなどが用いられる。

【００５０】なお、ネットワーク管理システムが管理する対象機器を、ここでは被管理機器と呼ぶ。この被管理機器は電子計算機、端末、ネットワーク機器、周辺機器、ケーブル類、設備機器の６つに分類する。

【００５１】電子計算機は、ワークステーションやパーソナルコンピュータやホストコンピュータやファイルサーバなどである。

【００５２】端末は、X端末やキャタクタ端末やグラフィック端末などである。

【００５３】ネットワーク機器は、ルータやリピータやターミナルサーバやトランシーバやブリッジやプロトコルコンバータやモデムなどである。

【００５４】周辺機器は、プリンタやワードプロセッサやファクシミリやスキャナなどである。

【００５５】ケーブル類は、イーサネットケーブルや電話線や電源ケーブルなどである。

【００５６】設備機器は空調やフロアレイアウトや建屋地図などである。

【００５７】また、ネットワークとは、被管理機器が接続されていて、各機器間で通信が行われているものである。

【００５８】例えば、ワークステーション固有の属性としてＣＰＵ名、処理速度、クロック数、稼働ＯＳ、外部インターフェイス、ＭＡＣアドレス、論理マシン名、ＩＰアドレス、メモリサイズ、ハードディスク容量、増設ボードなどがあり、ルータ固有の属性には対応プロトコル、通信速度、ポート数、ポート形状、インターフェイス種類、拡張可能スロット数などがある。

【００５９】ソフトウェア固有の属性には、製品名、バージョン、稼働ＯＳ、稼働環境、マニュアル、インストールマシン、保管場所、機能概要、バージョンアップ費用などが挙げられる。

【００６０】ここに挙げた情報は、予め製品データベースに登録しておき、製品名と機種名を指定すれば必要な情報が得られるようになっている。

【００６１】上述のような製品に関する情報以外に、ネ

ットワーク管理システムは、個々のコンピュータやネットワーク機器に固有の購入価格、購入先、購入年月、シリアル番号、修理履歴、保守費用なども管理属性として保持する。

【００６２】さらに、ネットワーク管理システムは被管理機器である電子計算機や端末やネットワーク機器に関するソフトウェア環境、マシン環境、システム構成、ネットワークトラフィックなども管理属性として扱う。

【００６３】また、本発明のネットワーク管理システムで扱う被管理機器の属性には、設備情報における地番、建屋名、フロア、面積、机位置、座席、マシン位置なども含まれる。

【００６４】さらに、本発明のネットワーク管理システムでは以下に述べる手段を有する。

（１）ネットワーク設備データベース・インターフェイス

上述の対象となる被管理機器や各々の属性情報をデータベース化し、登録及び検索を行う。

【００６５】この場合、各々の製品に固有の情報であるシリアル番号、保守契約の有無、購入先、保守契約などは、新規購入時にデータベース登録する。また、これらの属性情報データベースへのアクセス用ユーザインターフェイスがあり、どの端末からでも、どのデータに対しても同じようなインターフェイスで入力や更新が可能である。

【００６６】（２）地図データベース

ＣＡＤベースの図形処理を用いて、全国規模の地図情報からビル内のフロア単位の建屋図面まで階層化して保存する。上述のネットワーク設備データベースとリンクさせ、画面に表示した地図で機器の情報もアクセスできるユーザインターフェイスを提供する。

【００６７】（３）ハードウェア配置及びネットワーク配線管理

ネットワークの配線、接続状況、電源配置、マシンレイアウト、電話配線等を地図データベースに格納されている地図に基づいて作成する。

【００６８】（４）システム構成管理

新規にコンピュータを購入する場合に、必要な機器構成やソフトウェアの一覧を生成し、目的に合ったシステム構成になっているかチェックする。

【００６９】（５）マシン環境管理

例えば、ホームディレクトリはどこか、どのディスクに何が入っているか、マシンのシステム構成はどうなっているか、誰がアカウントを持っているか等の情報検索を可能にする。

【００７０】（６）ネットワーク環境管理

物理的な意味でのネットワーク環境の管理を行う。どこに、どんなマシンや端末が接続しているか、イーサネットでのネットワーク基準を満たしているかなどをチェックする。

【００７１】（７）ソフトウェア管理

ネットワーク上に接続された電子計算機及びネットワーク機器で稼働するソフトウェアの製品名、バージョン、稼働ＯＳ、稼働環境、マニュアル、インストールマシン、保管場所、機能概要、バージョンアップ費用などのソフトウェアに関する属性の管理を行う。

【００７２】（８）物品在庫管理

未使用ケーブル、コネクタ、トランシーバ、ターミネータ等の数や貸し出しリストを管理する。

【００７３】（９）統計処理

通信プロトコルレベルのネットワーク管理ツールと連動させ、定常的なネットワーク状況を監視し、ネットワークトラフィック、マシンのロードアベレージ、プリンタ稼働状況などの統計をとる。

【００７４】（１０）ネットワーク敷設サポート

ネットワークの増設、機器追加、位置変更の際に、物理的なレベルで可否を診断する。例えば、電源供給量の過不足、コンセント数、イーサの制限長、接続可能な端末数などのチェックを行う。

【００７５】（１１）ネットワーク監視

診断型エキスパートシステムと連動させ、障害発生時に障害箇所の特定を行ったり、回復のための対策指示を行う。また、ネットワークに接続されているマシンや端末を管理プロトコルの利用により自動検知する。さらに、ホストマシンやネットワークの負荷測定の分析結果から障害発生前に異常を検知し、ネットワーク管理者にアラーム通知する。

【００７６】（１２）ネットワークインテグレイト

ここまでに述べたネットワークに関する情報を総合的に判断し、円滑なネットワーク運営に何が不足しているか、どうすれば効率良いネットワークになるかのアドバイスを行う。

【００７７】ここで、本実施例で扱う用語、ネットワーク構成について説明しておく。

【００７８】ネットワーク構成とは、電子計算機、端末、ネットワーク機器、周辺機器、ケーブル類がどのように接続しているかを示すものである。実際の接続の位置関係や距離などを含む接続状況を示すものを物理的ネットワーク構成、サブネットやセグメントといった論理的な単位での接続状況を示すものを論理的ネットワーク構成と呼ぶ。

【００７９】論理的なネットワーク構成図の例を図２に示す。図２の２００は通信網、２０１は電子計算機、２０２はネットワーク機器、２０３は端末である。

【００８０】一部の電子計算機には、ネットワークに接続されている別の電子計算機から送られてきた命令を実行し、その結果を送り返す機能がある。ネットワーク管理システムは、この機能を利用することで、ネットワークに接続されている電子計算機から情報を収集することができる。以下では、これを遠隔操作と呼ぶ。

【００８１】次に、本実施例で用いるネットワーク構成図面について説明する。

【００８２】ネットワーク構成図面とは、前記物理的ネットワーク構成と前記論理的ネットワーク構成を統括した図面であり、ある縮尺の地図、建屋図面、フロア図面上に、ネットワーク管理システムが管理する被管理機器を配置させ、同時にケーブル類の敷設状況や電源配置や電話配置なども含め、ネットワークの物理的な接続状況を実際の距離及び面積と合わせて表現したものである。

【００８３】前記ネットワーク構成図面は、図示したい位置、範囲、被管理機器、セキュリティレベル、目的などに応じ、図１の補助記憶装置１０５内にあるデータベースに格納された物理的ネットワーク構成、論理的ネットワーク構成、ネットワーク配線、フロア図面、地図、ネットワークトラフィックの統計情報、ネットワーク回線使用率等の中から必要な情報を検索した上で、求められる情報を統合し、図１の出力装置１０４に表示される図面である。

【００８４】本実施例で用いるネットワーク構成図面の例を図３に示す。

【００８５】図３において、３００は通信網、３０１はネットワーク機器、３０２は電子計算機、３０３は端末である。

【００８６】ネットワーク管理システムは、上述の管理属性に関する情報を格納したデータベース以外に、以下に述べるデータベースをさらに有している。

【００８７】図４は被管理機器の情報を格納したデータベース４０の構造を示したものであり、４００の被管理機器ＩＤは被管理機器を一意に決めることのできる番号である。

【００８８】この被管理機器ＩＤ４００は、ネットワーク管理システムが表示するネットワーク構成図面の被管理機器図形データに割り当てられている。

【００８９】４０１の接続情報は、物理的に直接接続している被管理機器の被管理機器ＩＤである。

【００９０】４０２の分類は、電子計算機、端末、ネットワーク機器、周辺機器、ケーブル類を識別するものである。

【００９１】４０３の遠隔操作は、遠隔操作の可能な被管理機器であるか判別する項目である。

【００９２】４０４の管理者は、被管理機器を管理しているユーザのログイン名である。管理者は複数の場合もある。

【００９３】図５はネットワーク環境を維持するために必要なファイル名の一覧が登録されているデータベース５０の構造を示すもので、このデータベース５０に格納している情報は、ネットワーク管理者であるネットワーク管理システムの使用者により予め登録されている。

【００９４】ネットワーク上での被管理機器間の通信は、通信データを一定の長さに区切った情報単位により行われている。これをパケットと呼ぶ。

【００９５】図６にパケットの構成を示す。パケットは大きく２つの部分に分けることができる。すなわち、送受信するために必要な制御情報を格納しているヘッダ部６０と実際に送受信したい情報を格納したデータ部６１である。ヘッダ部６０には、各種の制御情報が格納されているが、本発明の一実施例にかかるヘッダ情報は図示のように、受信先の被管理機器ＩＤ６００、送信元の被管理機器ＩＤ６０１、パケットサイズ（バイト数）６０２、通信プロトコル６０３で構成されている。

【００９６】ここから、被管理機器である電子計算機が、複数の別な電子計算機から遠隔ログインやファイル転送などでアクセスされている状態を表示する処理について、図７のフローチャートに沿って説明する。

【００９７】ネットワーク上の遠隔処理が可能な全ての電子計算機は、常時ネットワークインタフェース上を送受信されるパケットのヘッダ部の一部を収集し記録している。これは、ネットワーク管理システムの遠隔操作として実行されている。

【００９８】まず、ステップ７００において、ネットワーク管理システムは、出力装置１０４にネットワーク構成を表示している。

【００９９】ステップ７０１において、使用者により入力装置１０３から監視対象の電子計算機を指定する。

【０１００】次にステップ７０２において監視期間を指定し、さらにステップ７０３において監視対象の電子計算機の被管理機器ＩＤを用いて被管理機器情報を図４のデータベース４０より検索する。

【０１０１】続く、ステップ７０４において、指定された電子計算機は遠隔操作が可能かどうかを調査する。遠隔操作が可能であれば、ステップ７０５へ、不可能であれば処理を終了する。

【０１０２】ステップ７０５においては、指定された電子計算機の被管理機器ＩＤを用いて、ステップ７０２で指定された期間に収集したデータをネットワーク管理システムに送信する遠隔操作を実行する。

【０１０３】この時の収集データは、受信先被管理機器ＩＤ６００、送信元被管理機器ＩＤ６０１、通信プロトコル６０３である。

【０１０４】図８に収集データの例を示す。８００は受信先被管理機器ＩＤ、８０１は送信元被管理機器ＩＤ、８０２は通信プロトコルを示している。

【０１０５】次にステップ７０６において、出力装置１０４にステップ７０５で送信された収集データを結果として表示する。

【０１０６】次に、被管理機器を流れているパケットの通信プロトコル別の数量や数量比を表示する処理について図９のフローチャートに沿って説明する。

【０１０７】ネットワーク上の遠隔処理が可能な全ての電子計算機は、常時ネットワークインタフェース上を送

受信されるパケットのヘッダ部の一部を収集し記録している。これは、ネットワーク管理システムの遠隔操作として実行されている。

【０１０８】ステップ９００において、ネットワーク管理システムは、出力装置１０４にネットワーク構成を表示している。次にステップ９０１において、使用者により入力装置１０３から監視対象の被管理機器を指定され、続くステップ９０２において使用者により監視期間が指定される。

【０１０９】ステップ９０３において、ステップ９０１で指定された被管理機器の被管理機器ＩＤを用いて被管理機器情報を図４に示したデータベース４０より検索する。

【０１１０】ステップ９０４において、検索した被管理機器が遠隔操作可能かどうかを調査する。

【０１１１】遠隔操作が不可能であればステップ９０５へ、可能ならばステップ９０６へ処理を進める。

【０１１２】ステップ９０５において、ステップ９０４で調べた被管理機器の接続情報を用いて、被管理機器の被管理機器情報を図４に示したデータベース４０より検索する。

【０１１３】接続情報として複数の被管理機器ＩＤがある場合は、先頭の被管理機器ＩＤが使用される。

【０１１４】遠隔操作可能な被管理機器が見つかるまでステップ９０４、９０５の処理を繰り返す。

【０１１５】ステップ９０６において、ステップ９０４で検索した被管理機器の被管理機器ＩＤを用いて、ステップ９０２で指定された期間に収集したデータをネットワーク管理システムに送信する遠隔操作を実行する。

【０１１６】この時の収集データは、パケットサイズ、通信プロトコルである。図１０に収集データの例を示す。１０００はパケットサイズ、１００１は通信プロトコルである。

【０１１７】ステップ９０７において、図１０の収集データより、通信プロトコル別にパケットサイズの合計を算出する。

【０１１８】ステップ９０８において、ステップ９０７で算出した通信プロトコル別パケットサイズの合計より、通信プロトコルのパケットサイズの総計を算出する。

【０１１９】ステップ９０９において、ステップ９０７の通信プロトコル別合計をステップ９０８の総計で割り、その数量比を算出する。

【０１２０】ステップ９１０において、出力装置にステップ９０７の結果とステップ９０９の結果をグラフで表示する。図１１は棒グラフを用いた通信プロトコル別のパケット数量の合計の表示例、図１２は円グラフを用いた通信プロトコル別のパケットの数量比の表示例を示すものである。なお、この他の表示形式をとってもよい。

【０１２１】次に、特定の端末や電子計算機の表示装置（ここでは、まとめて端末と呼ぶ）で、どのユーザ名で、どこの電子計算機にログインしているか、という情報を調査し表示する処理を、図２、図３、図１４、図１５を参照しながら図１３のフローチャートにそって説明する。

【０１２２】図１４はログイン記録テーブル１４０である。これは、各電子計算機へのログインを記録するテーブルであり、各電子計算機が保持している。このログイン記録テーブル１４０は、ログインしたユーザ名１４００、そのログインで使用した仮想端末名１４０１、ログインした端末名１４０２、ログインした時刻１４０３、ログアウトした時刻１４０４、ログインする前のユーザ名（あるユーザにログインしてからログアウトせずにそこからユーザ名１４００でログインした場合）１４０５が格納されている。ログイン中である場合、ログアウトした時刻１４０４は空欄である。

【０１２３】図１５は、指定した端末で、どのユーザ名で、どこの電子計算機にログインしているかを示す検出結果の表示例であり、電子計算機名１５００、ログインしたユーザ名１５０１、そのログインで使用した仮想端末名１５０２、ログインした時刻１５０２が表示される。

【０１２４】まず、ステップ１３００において、図２に示すような論理的なネットワーク構成図あるいは図３に示すような物理的なネットワーク構成図を表示する。

【０１２５】次にステップ１３０１において、システムのユーザにより調査したい端末２０３が指定される。

【０１２６】次にステップ１３０２において、システムはネットワーク内の各電子計算機のログイン記録テーブル１４０を調査し、ステップ１３０１で指定された端末２０３からのログイン項目を検出する。

【０１２７】ステップ１３０２で検出するのはログイン中のもの（図１４の１４０４が空欄のもの）である。また、仮想端末とは電子計算機側から見た論理的な端末（実際には１つの端末であるが、ソフトウェアでは複数の端末として扱うことをいう。例えば、複数のウインドウのそれぞれを１つの端末として使用する場合に相当する。）意味し、一つのログインに対し一つの名前で割り当てられる。例えば、ある端末から複数ログインした場合、電子計算機側は複数の端末からログインされたと仮想して端末名を割り当てる。その個々の仮想的な端末を仮想端末と呼ぶ。

【０１２８】次に、ステップ１３０３において、システムは１３０２で検出した項目について、図１５に示すように、電子計算機名１５００、ユーザ名１５０１、仮想端末名１５０２、ログインした時刻１５０３をリストにして表示する。

【０１２９】次に、ネットワーク環境を維持していくために必要なファイルのアクセス履歴を監視する処理について図１６、１７のフローチャートに沿って説明する。

【０１３０】ネットワーク管理システムが、予め、アクセス履歴を保存するために実行している処理について図１６のフローチャートに沿って説明する。

【０１３１】ステップ１６００において、ネットワーク管理システムは、使用者によりアクセス履歴の保存期間を指定される。次に、ステップ１６０１において、図４に示したデータベース４０より、遠隔操作可能な電子計算機の被管理機器情報を全て検索する。

【０１３２】ステップ１６０２において、検索した全ての遠隔操作可能な電子計算機の被管理機器ＩＤを用いて、図５に示したデータベース５０に登録されているファイルへのアクセス履歴情報を、ステップ１６０１で指定された期間、遠隔操作を行う電子計算機に保存する遠隔操作を実行する。

【０１３３】図１８にアクセス履歴情報１８０の例を示す。ここで、１８０１はアクセスユーザ、１８０２はアクセス方法、１８０３はアクセス日時である。

【０１３４】次に、アクセス履歴を表示する処理について図１７のフローチャートに沿って説明する。

【０１３５】ステップ１７００において、ネットワーク管理システムは出力装置にネットワーク構成を表示している。ステップ１７０１において、使用者により入力装置で監視する電子計算機が指定される。ステップ１７０２において、指定された電子計算機の被管理機器ＩＤを用いて被管理機器情報を図４に示したデータベース４０より検索する。

【０１３６】ステップ１７０３において、指定された電子計算機が遠隔操作可能かどうかを調査する。遠隔操作ができればステップ１７０４へ、できなければ処理を終了する。

【０１３７】ステップ１７０４において、遠隔操作可能な電子計算機の被管理機器ＩＤを用いて、図５に示したデータベース５０のファイルのアクセス履歴情報をネットワーク管理システムに送信する遠隔操作を実行する。

【０１３８】ステップ１７０５において、ステップ１７０４においてネットワーク管理システムに送信されたアクセス履歴情報を出力装置に表示する。表示例を図１９に示す。

【０１３９】次に、特権モードで稼働しているプログラムを捜し出して表示する処理を、図２、図３、図２１、図２３を参照して図２０のフローチャートにそって説明する。

【０１４０】図２１はプログラム起動ログテーブル２１０である。このプログラム起動ログテーブル２１０は、各電子計算機で起動されたプログラムの情報を記録するテーブルであり、各電子計算機が保持している。プログラム起動ログテーブルには図示のように、起動したユーザ名２１００、起動されたプログラム名称２１０１、起動した仮想端末名２１０２、起動した端末名２１０３、起動時刻２１０４、終了時刻２１０５、起動時のモード２１０６が格納されている。稼働中である場合、終了時刻２１０５は空欄である。

【０１４１】図２２は特権モードで稼動中のプログラムを検出した結果の表示例であり、プログラム名２２００、ユーザ名２２０１、起動した仮想端末名２２０２、起動した端末名２２０３、起動時刻２２０４が表示される。

【０１４２】特権モードのプログラムとは、他のプログラムやファイルに対して特権的な動作のできるプログラムである。特権的な動作の例としては、一般のユーザに対して書き込みを禁止しているファイルの書き換え動作や、他のユーザが起動しているプログラムの停止動作がある。

【０１４３】まずステップ２０００において、図２に示したような論理的なネットワーク構成図、あるいは図３に示したような物理的なネットワーク構成図を表示する。

【０１４４】次に、ステップ２００１において、システムのユーザにより調査したい電子計算機が指定される。

【０１４５】次に、ステップ２００２において、ステップ２００１で指定された電子計算機が有する図２１に示すような全プログラム起動ログテーブルを調査し、特権モードで稼働しているプログラムを検出する。

【０１４６】ステップ２００２で検出するのは、終了時刻が空欄であるもの、即ち、稼働中のものである。

【０１４７】次に、ステップ２００３において、システムはステップ２００２で検出したプログラムについて、プログラム名称２２００、プログラムを起動したユーザ名２２０１、プログラムを起動した仮想端末名２２０２、プログラムを起動した端末名２２０３、プログラムの起動時刻２２０４をリストにして図２２に示すように表示する。

【０１４８】次に、指定されたある期間中に、誰がどこで特権ユーザとなり、どのようなプログラムを動かしたかを調査し、表示する処理を図２、図３、図１４、図２１、図２４、図２５を参照して図２３のフローチャートにそって説明する。

【０１４９】図２４には、指定した期間内に、どのユーザ名からどの期間、特権ユーザにログインしていたかを表すテーブル２４０である。このテーブル２４０は、図２３のフローチャートの処理途中で作成される。図２４において、２４００は仮想端末名、２４０１は端末名、２４０２はログインしていた時間帯、２４０３は特権ユーザにログインしたユーザ名である。指定された調査開始時刻以前に特権ユーザとしてログインしている場合は、調査開始時刻をログインした時刻として扱う。また、調査終了時刻以後に特権ユーザからログアウトしている場合は、調査終了時刻をログアウトした時刻として扱う。

【０１５０】図２５は、ある期間に誰がどの端末で特権

ユーザとなり、どのようなプログラムを作動させたかを検出した結果の表示例であり、仮想端末名２５００、ログインした端末名２５０１、起動時刻２５０３、終了時刻２５０４、ログインしたユーザ名２５０５が表示される。

【０１５１】電子計算機にログインする場合、通常の電子計算機利用を目的としたログイン名（以降では、これを一般ユーザと呼ぶ）か、電子計算機の管理を目的としたログイン名（以降では、これを特権ユーザと呼ぶ）のどちらかを使用する。

【０１５２】特権ユーザでログインすると、電子計算機上の全てのプログラムの起動や強制終了、全てのテーブル類の書き換えや消去などの特権的な動作が行える。

【０１５３】まずステップ２３００において、図２に示したような論理的なネットワーク構成図、あるいは図３に示したような物理的なネットワーク構成図を表示する。

【０１５４】次にステップ２３０１において、システムのユーザにより調査したい電子計算機名と調査期間が指定される。

【０１５５】次に、ステップ２３０２において、システムはステップ２３０１で指定された電子計算機のログイン記録テーブル１４０（図１４）を調査し、仮想端末名１４０１、端末名１４０２、ステップ２３０１で指定した期間において特権ユーザがログインした時間帯１４０３と１４０４、特権ユーザでログインする前のユーザ名１４０５を検出し、図２４に示すような検出結果リストを作成する。

【０１５６】次に、ステップ２３０３において、ステップ２３０２で作成した検出結果リスト（図２４）が空であるかを判断する。

【０１５７】ステップ２３０３が偽である場合は、ステップ２３０４において、検出結果リストの先頭項目の情報の特権ユーザがログインしていた時間帯と仮想端末名を用いて、時間帯２４０２に仮想端末２４００で起動されたプログラムを、プログラム起動ログテーブル２１０（図２１）から検出する。

【０１５８】ステップ２３０５において、ステップ２３０４で使用した先頭項目をステップ２３０２で作成した検出結果リストから削除し、ステップ２３０３に戻る。

【０１５９】ステップ２３０３が真である場合は、ステップ２３０５において、システムはステップ２３０４で検出した結果をまとめて図２５に示すように仮想端末名２５００、ログインした端末名２５０１、起動したプログラム名称２５０２、プログラム起動時刻２５０３、プログラム終了時刻２５０４、ログインしたユーザ名２５０５をリストにして表示する。

【０１６０】次に、ネットワーク環境を維持していくために必要なファイルのアクセス権の設定を検査する処理について、図２７～図３０を参照し、図２６のフローチャートに沿って説明する。

【０１６１】ネットワーク管理システムは、ファイルのアクセス権を、ファイル所有者、グループ所有者、その他の所有者のレベルに分けて行う。ファイル所有者は、ユーザ、グループ所有者はグループ、その他の所有者はファイル所有者、グループ所有者以外のユーザを示す。

【０１６２】ここでグループとは、複数のユーザをなんらかの目的でひとまとめにしたもので、例えば、あるプログラムの開発プロジェエクトの全構成員とか、職制上の部長全員といったものになる。

【０１６３】ネットワーク管理システムは、ネットワーク環境を維持するため必要なファイルの本来あるべきアクセス権が登録されているデータベースを持っている。そのデータベース２７０を図２７に示す。図２７において、２７００はファイル名、２７０１はファイル所有者に対するアクセス権、２７０２はグループ所有者に対するアクセス権、２７０３は上記以外のユーザに対するアクセス権、２７０４はファイル所有者、２７０５はグループ所有者を示している。

【０１６４】ここで例示しているファイルは、以下の設定を行う環境維持ファイルである。

【０１６５】まず、ファイル名２７００の「／ｅｔｃ／ｐａｓｓｗｄ」はネットワークを使用する全ユーザが登録しているファイル名である。また、「ｅｔｃ／ｇｒｏｕｐ」はユーザが属することができる全グループを登録しているファイル名である。さらに、「／ｅｔｃ／ｈｏｓｔｓ」はネットワーク上の電子計算機、ネットワーク機器、周辺機器を登録しているファイル名である。

【０１６６】図２８はアクセス権の設定を説明する概念図であり、２８００は読み、２８０１は書き、２８０２は実行のアクセス権を示すフィールドであり、ビットが１の時、許可されている。この図示の例では、読み、書きは許されているが、実行は許されていない。

【０１６７】図２６のステップ２６００において、ネットワーク管理システムは使用者により、ファイルのアクセス権の設定を検査する時間間隔、例えば１時間おき、３日間おき等の期間が指定される。

【０１６８】ステップ２６０１において、図４に示したデータベース４０から、遠隔操作可能で、かつ電子計算機の管理者がネットワーク管理システムの使用者と同一のものを検索する。

【０１６９】ステップ２６０２において、ステップ２６０１で検索した全ての電子計算機に対して、被管理機器ＩＤを用いて図５に示したデータベース５０に格納されているネットワーク環境維持ファイルのアクセス権の設定状況を、ネットワーク管理システムに送信する遠隔操作を実行する。

【０１７０】図２９はある電子計算機から送信されたアクセス権の設定状況の例である。

【０１７１】ステップ２６０３において、ステップ２６

０２で送信されたアクセス権の設定状況と図２７に示したデータベースのアクセス権とを比較し、図３０に示すような比較結果テーブル３００を作成する。

【０１７２】図３０において、３０００は被管理機器ＩＤ、３００１は比較を行ったネットワーク環境維持ファイル名、３００２は送信されたアクセス権の設定状況、３００３は本来あるべきアクセス権である。

【０１７３】比較の結果、相違がない場合は、被管理機器ＩＤ３０００とファイル名３００１のみが格納される。

【０１７４】次にステップ２６０４において、被管理機器の管理者に対して、ステップ２６０３で作成した比較結果テーブル３００をメールで通知する。

【０１７５】ステップ２６０５において、ステップ２６００で指定された期間、検査期間の設定変更がないか待つ。そして、ステップ２６０６において、ステップ２６００で指定された期間情報が削除されるまでステップ２６０１からステップ２６０５の処理を繰り返す。

【０１７６】次に、一般ユーザが特権モードで起動できるプログラムを探し出して表示する処理を、図２，図３，図３２～図３４を参照し、図３１のフローチャートにそって説明する。

【０１７７】図３２は計算機中の全てのプログラムについてのプログラム状態テーブル３２０である。電子計算機には、一般モードで稼働するプログラムと特権モードで稼働するプログラムがある。またプログラムによって、所有者のみ起動可能、所有者と同じグループのユーザのみ起動可能など、起動者の制限もある。これらの稼働モードや起動者の制限に関する情報はプログラム状態テーブル３２０に格納されている。

【０１７８】プログラム状態テーブル３２０は図３２に示すように、プログラム毎のプログラム名称３２００、プログラムの所有者３２０１、起動可能なユーザ３２０２、稼働時のモード３２０３から成る。

【０１７９】このプログラム状態テーブル３２０は各電子計算機が保持している。

【０１８０】図３３は、特権モードで起動できても支障のないプログラムのテーブル３３０で、これはネットワーク管理者によって登録される。特権モードで起動できても支障のないプログラムが事前に明らかな場合は、ネットワーク管理者は予め特権モードで起動できても支障のないプログラムをテーブル３２０に構成してシステムに登録して置く。ここではこれを事前登録テーブルと呼ぶ。

【０１８１】図３４は一般ユーザが特権モードで起動できるプログラムについての検出結果の表示例である。

【０１８２】まず、ステップ３１００において、図２に示したような論理的なネットワーク構成図、あるいは図３に示したような物理的なネットワーク構成図を表示する。

【０１８３】次に、ステップ３１０１において、ネットワーク管理者により一般ユーザが特権モードで起動できるプログラムの存在を調査したい電子計算機が指定される。

【０１８４】次に、ステップ３１０２において、システムはその電子計算機内のプログラム状態テーブル３２０を調査し、稼働時のモード３２０３が特権モードであるプログラムを検出する。

【０１８５】次に、ステップ３１０３において、事前登録テーブル３３０が登録されているかを判断する。ステップ３３０３が真であれば、ステップ３３０４において、事前登録テーブル３３０に登録されているプログラムの項目を、ステップ３１０２の検出結果から削除する。

【０１８６】次に、ステップ３１０５において、ステップ３１０２で検出したプログラム、又はステップ３１０４において項目削除を行った後のプログラムについて、図３４に示すように、プログラム名称３４００、プログラムの所有者３４０１、誰によって起動できるか３４０２をリストにして表示する。

【０１８７】また、ステップ３１０５において、リスト表示をシステムの出力装置に行うのではなく、ネットワーク管理者にメールで通知するのも一つの表示方法とする。

【０１８８】次に、監視プログラムがネットワーク上のどの電子計算機で稼働しているかを調査して表示する処理を、図２，図３，図３６～図３９を参照し、図３５のフローチャートにそって説明する。

【０１８９】図３６は、どのような監視プログラムを起動させているかを示すテーブル３６０で、ネットワーク管理者が登録したものである。

【０１９０】監視プログラムとは、外部からの侵入や不審なプログラムの稼働を監視したり、その結果を管理者に通知したりするプログラムのことであり、ネットワーク管理者が各電子計算機で稼働するように設定している。ネットワーク管理者は予め、図３６に示すように、監視プログラムの稼働すべき電子計算機名３６００と、その電子計算機で稼働すべき監視プログラム名３６０１と、その監視プログラムの重要度３６０２を格納したテーブル３６０を作成してシステムに登録しておく。このテーブルを監視プログラム登録テーブル３６０と呼ぶ。

【０１９１】図３７、図３８は調査対象指定の例、図３９は監視プログラムが全て稼動中かの調査結果の表示例である。

【０１９２】まずステップ３５００において、図２に示したような論理的なネットワーク構成図、あるいは図３に示したような物理的なネットワーク構成図を表示する。

【０１９３】次に、ステップ３５０１において、システムのユーザにより監視プログラムが稼働しているかどう

かを調査するように指示される。調査対象の指示は、図３７に示すような電子計算機３７００の特定や、図３８に示すような範囲指定３８００などにより行う。

【０１９４】次に、ステップ３５０２において、指定された各電子計算機上でプログラム起動ログテーブル２１０（図２１）を調査し、監視プログラム登録テーブル３６０（図３６）に含まれるプログラムの稼働状況を検出する。

【０１９５】ステップ３５０３において、ステップ３５００で表示したネットワーク構成図上で、指定された監視プログラムが全て稼働している電子計算機と、稼働していない監視プログラムのある電子計算機の違いが判るように表示する。例えば、図３９に示すように、監視プログラムが全て稼働している電子計算機は符号３９００のように斜線で表示し、稼働していない監視プログラムのある電子計算機は符号３９０１のように枠のみで表示するといった方法や、色を変えたり、表示輝度を変えるなどの方法により、違いが判るように表示する。

【０１９６】次に、ステップ３５０４において、図３６のテーブル３６０で重要度３６０２が「大」と指定されている監視プログラムが全て稼働中であるかどうかを、ステップ３５０２の検出結果と監視プログラム登録テーブル３６０（図３６）との比較により調査し、ステップ３５０４が偽である場合は、ステップ３５０５において、「重要度大」と指定されている監視プログラムが稼働していない旨を、メールや電話などで管理者へ直接通知する。

【０１９７】次に、ネットワーク管理システムがネットワーク上のセキュリティホールを検出後、検出したセキュリティホールへの対策を行う処理を、図４０～図４４を用いて、図４５のフローチャートに沿って説明する。

【０１９８】図４０はセキュリティホールテーブル４００の内容を示す図である。セキュリティホールには、その内容に応じてセキュリティＩＤとセキュリティ対策ＩＤが付けられている。図４０の４０００はセキュリティＩＤ、４００１はセキュリティホール内容、４００２はセキュリティ対策ＩＤである。

【０１９９】図４１はセキュリティ対策テーブル４１０の内容を示す図である。このセキュリティ対策テーブル４１０には、セキュリティ対策ＩＤ４１００と、セキュリティホールに対するチェック条件４１０１と、チェック条件４１０１がＹＥＳの場合の処理内容を表すＹＥＳ処理番号４１０２と、チェック条件４１０１がＮＯの場合の処理内容を表すＮＯ処理番号４１０３が格納されている。

【０２００】あるセキュリティホールに対するチェック条件が複数必要な場合には、このＹＥＳ処理番号とＮＯ処理番号に、セキュリティ対策ＩＤが格納される場合もある。

【０２０１】図４２はＹＥＳ／ＮＯ処理テーブル４２０の内容を示す図である。このＹＥＳ／ＮＯ処理テーブル４２０は、処理番号４２００、処理内容４２０１となる。

【０２０２】図４３は管理テーブル４３０の内容を示す図である。この管理テーブル４３０には、ネットワーク管理システムの管理対象であるネットワークの管理者が登録されている。

【０２０３】図４３において、４３００は管理者のＩＤ、４３０１は管理名、４３０２は管理者の所属である。

【０２０４】図４４は外部ユーザテーブル４４０の内容を示す図である。この外部ユーザテーブル４４０には、ネットワーク管理システムの管理対象外である外部ネットワークから、管理対象のネットワークに対して、アクセスを許諾されている外部ユーザが登録されている。

【０２０５】図４４において、４４００は外部ユーザのＩＤ、４４０１は外部ネットワーク名、４４０２はユーザ名、４４０３はユーザの所属である。

【０２０６】まず、ネットワーク管理システムは、上述の実施例に示したような処理、即ち、常時ネットワーク環境を監視し、セキュリティホールを検出し、ネットワーク構成画面上に検出したセキュリティホールの表示を行う処理と同時に、セキュリティホールを後述するセキュリティ対策処理に通知する機能を有する。従って、これから述べるセキュリティホールへの対策を行う処理は、このセキュリティ対策処理への通知が発生した時点から処理を開始する。

【０２０７】図４５のフローチャートのステップ４５００において、検出したセキュリティホールのセキュリティＩＤの通知を受け取る。次に、ステップ４５０１において、通知されたセキュリティＩＤを元に図４０に示したセキュリティホールテーブル４００を検索し、該当するセキュリティ対策ＩＤを得る。

【０２０８】次に、ステップ４５０２において、ステップ４５０１で得たセキュリティ対策ＩＤを元に、図４１で示したセキュリティ対策テーブル４１０を検索し、セキュリティホールに対応したチェック条件を得る。

【０２０９】ステップ４５０３において、チェック条件がＹＥＳかどうかを判断する。その際、必要に応じて図２１のプログラム起動ログテーブル２１０によりプロセスの稼働状況を確認したり、図４３の管理者テーブル４３０によりセキュリティホールを発生させたのが管理者かどうか調査したり、図４４の外部ユーザテーブル４４０によりアクセスを許諾された外部ユーザかどうかを調査したりする。

【０２１０】ステップ４５０３のチェック条件がＹＥＳだった場合は、ステップ４５０４において、ＹＥＳ処理に格納されている内容がセキュリティ対策ＩＤの場合は、再度セキュリティ対策テーブル４１０の検索を行うために、ステップ４５０２の前に戻る。ＹＥＳ処理に格

納されている内容が処理番号になるまでこれを繰り返す。

【０２１１】ＹＥＳ処理に処理番号が格納されていると、次に、ステップ４５０５でその処理番号を元に図４２ＹＥＳ／ＮＯテーブル４２０を検索する。

【０２１２】また、ステップ４５０３のチェック条件がＮＯだった場合も同様に、ステップ４５０６において、ＮＯ処理に格納されている内容がセキュリティ対策ＩＤの場合は、再度セキュリティ対策テーブル４１０の検索を行うために、ステップ４５０２の前に戻る。ＮＯ処理に格納されている内容が処理番号になるまでこれを繰り返す。

【０２１３】ＮＯ処理に処理番号が格納されていると、次に、ステップ４５０７でその処理番号を元に図４２のＹＥＳ／ＮＯ番号テーブル４２０を検索する。

【０２１４】ステップ４５０５、又はステップ４５０７でＹＥＳ／ＮＯ処理テーブル４２０を検索して処理内容を得ると、次に、ステップ４５０８において、処理内容を実行してセキュリティ対策を行う。

【０２１５】

【発明の効果】以上説明したように、本発明においては、

（１）ソフトウェア的セキュリティホールを検出し、検出したソフトウェア的セキュリホールをネットワーク構成図面上に表示するので、ネットワークにおけるセキュリティを確保することができる。

【０２１６】（２）また、ネットワーク及びネットワーク機器に対するアクセス状況を常時監視するので、外部からの侵入、内部での不正利用の発見を速やかに行うことができる。

【０２１７】（３）さらに、ネットワーク環境設定用ファイルの内容をアクセス許諾条件に基づき照合及び検査するので、適正なネットワーク利用環境の構築を容易に行うことができる。

【０２１８】（４）さらに、ネットワーク管理の対象となっているネットワーク機器をネットワー構成図面上で識別可能な形式で表示させるので、安全なネットワーク環境を視覚的に簡単に把握することができる。

【図面の簡単な説明】

【図１】　本発明の一実施例にかかるネットワーク管理システムの構成を示すブロック図である。

【図２】　本実施例の論理的ネットワークの構成を説明するための摸式的構成図である。

【図３】　本実施例の表示装置上へのネットワーク構成図面の表示例を示す図である。

【図４】　本実施例の被管理機器ＩＤ、接続情報、分類、遠隔操作、管理者の対応を表す被管理機器の情報を格納したデータベースの構成を示す図である。

【図５】　本実施例のネットワーク環境を維持するために必要なファイルが登録されているデータベースの構成を示す図である。

【図６】　本実施例のパケットのヘッダ部の構造を説明するための摸式図である。

【図７】　本実施例の電子計算機がどの被管理機器からアクセスされているか表示する処理手順を示すフローチャートである。

【図８】　本実施例の電子計算機へのアクセス状況に関する収集データの例を示す図である。

【図９】　本実施例の被管理機器を流れているパケットの通信プロトコル別の数量や数量比を表示する処理手順を示すフローチャートである。

【図１０】　本実施例の被管理機器をながれているパケットのパケットサイズと通信プロトコルを収集したデータの例を示す図である。

【図１１】　本実施例の通信プロトコル別のパケットサイズ合計を示す棒グラフである。

【図１２】　本実施例の通信プロトコル別のパケットサイズ合計の数量比を円グラフを用いて表示した例である。

【図１３】　本実施例の指定した端末で、どのユーザ名でどこの電子計算機にログインしているかを調査して表示する処理手順を示すフローチャートである。

【図１４】　本実施例のログイン記録テーブルの例を示す図である。

【図１５】　本実施例の指定した端末で、どのユーザ名でどこの電子計算機にログインしているかを示す検出結果の表示例である。

【図１６】　本実施例のネットワーク環境維持ファイルへのアクセス履歴を保存するために、予め、実行する処理手順を示すフローチャートである。

【図１７】　本実施例のネットワーク環境維持ファイルへのアクセス履歴を表示する処理手順を示すフローチャートである。

【図１８】　本実施例のネットワーク環境維持ファイルへのアクセス履歴の例を示す図である。

【図１９】　本実施例のネットワーク環境維持ファイルへのアクセス履歴の表示例を示す図である。

【図２０】　本実施例の特権モードで稼働中のプログラムを捜し出して表示する処理手順を示すフローチャートである。

【図２１】　本実施例のプログラム起動ログテーブルの例を示す図である。

【図２２】　本実施例の特権モードで稼働中のプログラムを検出した結果の表示例を示す図である。

【図２３】　本実施例のある期間に誰がどの端末で特権ユーザとなり、どのようなプログラムを動かしたかを調査し表示する処理手順を示すフローチャートである。

【図２４】　本実施例のある期間に特権ユーザでログインした時間帯や端末名等をログイン記録テーブルから検出した結果の例である。

【図２５】　本実施例のある期間に誰がどの端末で特権ユーザとなり、どのうなプログラムを動かしたかを検出した結果の表示例である。

【図２６】　本実施例のネットワーク環境維持ファイルのアクセス権を検査する処理手順を示すフローチャートである。

【図２７】　本実施例のネットワーク環境維持ファイルのアクセス権の本来あるべき設定を表すデータベースの例を示す図である。

【図２８】　本実施例のアクセス権の設定を説明する概念図である。

【図２９】　本実施例のネットワーク環境維持ファイルのアクセス権を収集した例を示す図である。

【図３０】　本実施例のネットワーク環境維持ファイルのアクセス権を検査した結果の例を示す図である。

【図３１】　本実施例の一般ユーザが特権モードで起動できるプログラムを探し出して表示する処理手順を示すフローチャートである。

【図３２】　本実施例のプログラム状態テーブルの例を示す図である。

【図３３】　本実施例の事前登録テーブルの例を示す図である。

【図３４】　本実施例の一般ユーザが特権モードで起動できるプログラムを検出した結果の表示例である。

【図３５】　本実施例の監視プログラムが稼働しているかを調査して表示する処理手順を示すフローチャートである。

【図３６】　本実施例の監視プログラム登録テーブルの例を示す図である。

【図３７】　本実施例の調査対象となるコンピュータを指定する例を示す図である。

【図３８】　本実施例の調査対象の範囲を指定する例を示す図である。

【図３９】　本実施例の指定した監視プログラムが全て稼働中であるかどうかの表示例を示す図である。

【図４０】　本発明の一実施例にかかるネットワーク管理システムのセキュリティホールテーブルの内容を示す図である。

【図４１】　本発明の一実施例にかかるネットワーク管理システムのセキュリティ対策テーブルのないようを示す図である。

【図４２】　本発明の一実施例にかかるネットワーク管理システムのＹＥＳ／ＮＯ処理テーブルの内容を示す図である。

【図４３】　本発明の一実施例にかかるネットワーク管理システムの管理者テーブルの内容を示す図である。

【図４４】　本発明の一実施例にかかるネットワーク管理システムの外部ユーザテーブルの内容を示す図である。

【図４５】　本発明の一実施例にかかるネットワーク管理システムの検出したセキュリティホールへの対策を行う処理手順を示すフローチャートである。

【符号の説明】

１００…ネットワーク、１０１…通信制御装置、１０２…中央処理装置、１０３…入力装置、１０４…出力装置、１０５…補助記憶装置、２００…通信網、２０１…電子計算機、２０２…ネットワーク機器、２０３…端末、３００…通信網、３０１…ネットワーク機器、３０２…電子計算機、３０３…端末。

【図４】

図４

400 被管理機器ID	401 接続情報	402 分類	403 遠隔操作	404 管理者
000001	000010	電子計算機	○	mariko
023206	023207,023208	ケーブル類	×	taro
398730	398729,398731	ネットワーク機器	○	ant
⋮	⋮	⋮	⋮	⋮

40

【図５】

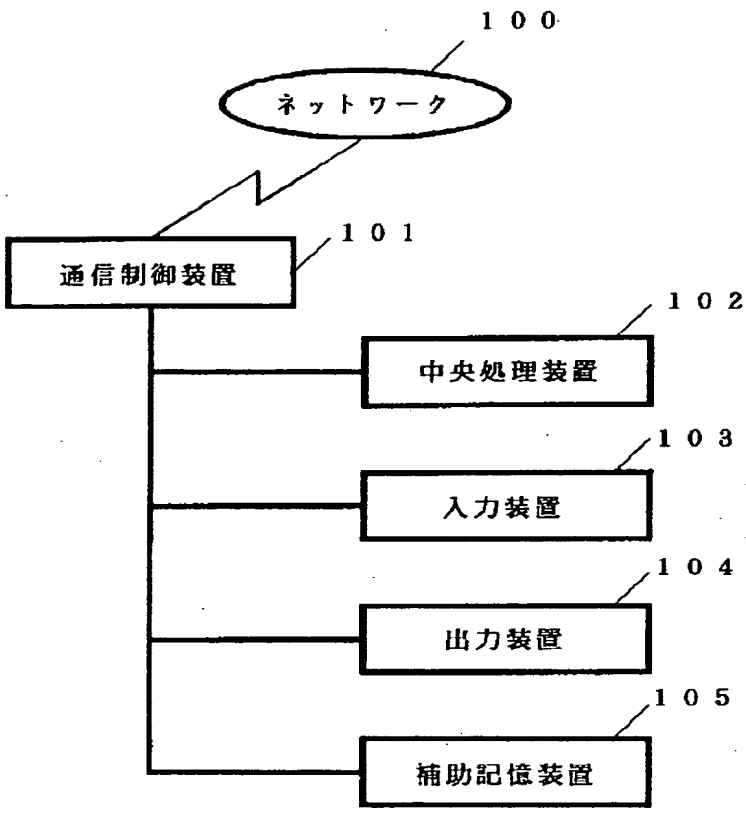
図５

ネットワーク環境維持ファイル
/etc/passwd
/etc/group
/etc/rc
⋮

50

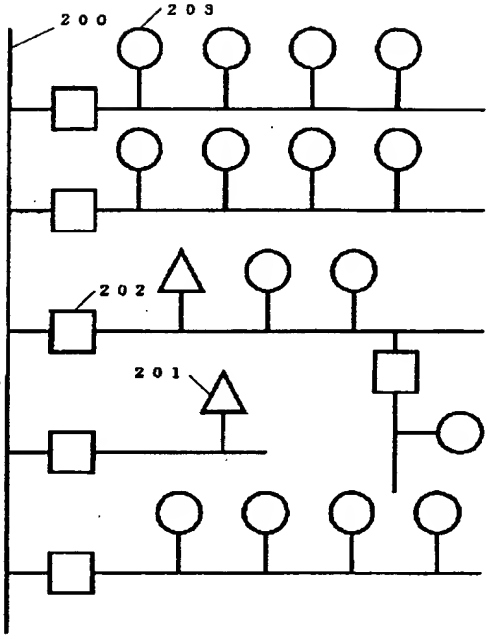
【図１】

図１



【図２】

図２



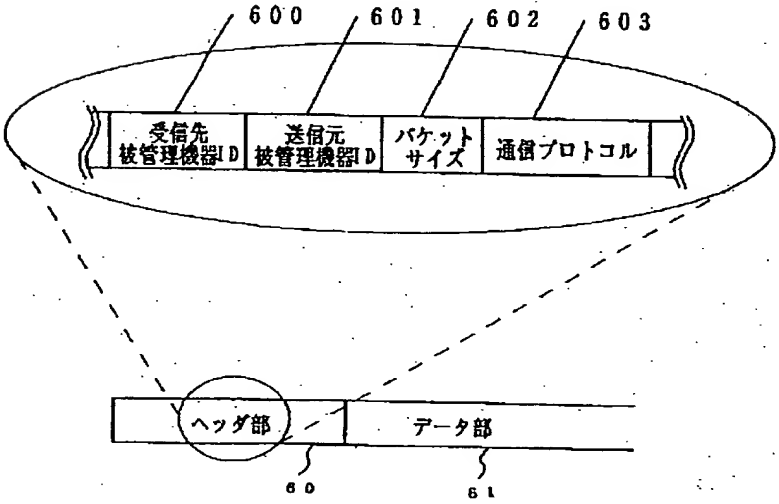
【図８】

図８

８００ 受信先被管理機器ID	８０１ 送信元被管理機器ID	８０２ 通信プロトコル
000001	002387	プロトコル１
874983	000001	プロトコル２
398730	000001	プロトコル３
⋮	⋮	⋮

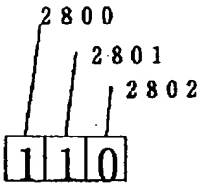
【図６】

図６



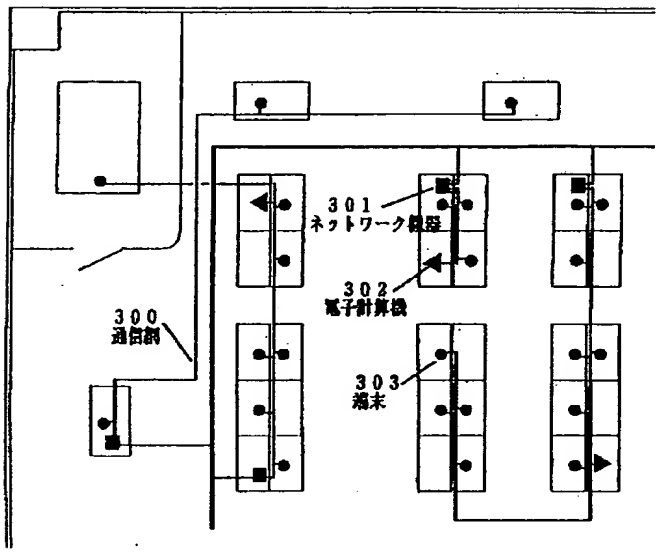
【図２８】

図２８



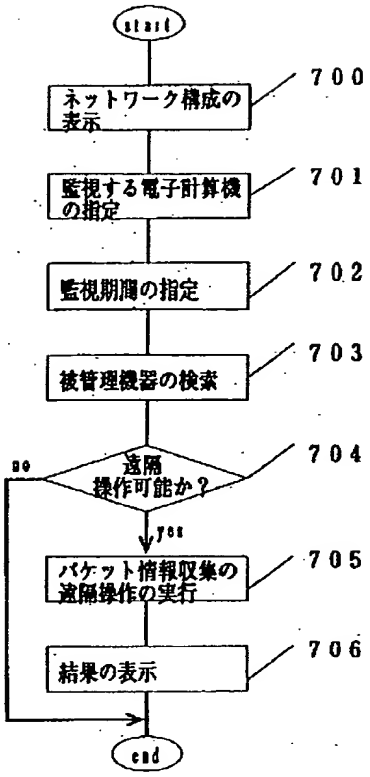
【図３】

図３



【図７】

図７



【図１０】

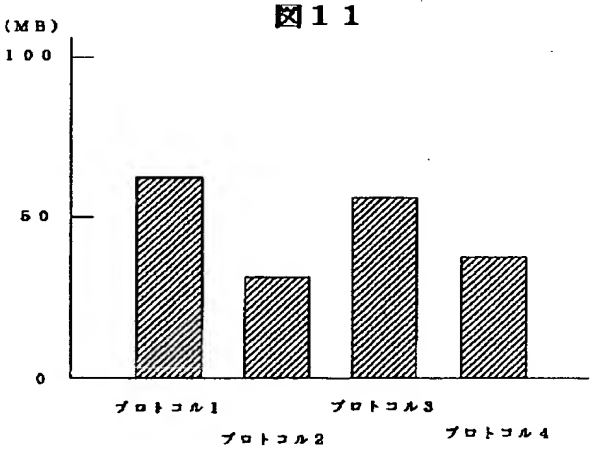
図１０

1000　1001

パケットサイズ	通信プロトコル
1500	プロトコル1
23	プロトコル2
125	プロトコル3
⋮	⋮

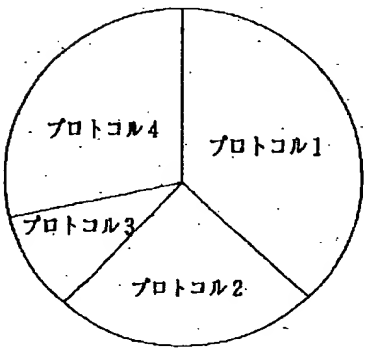
【図１１】

図１１



【図１２】

図１２



【図４３】

図４３

管理者テーブル

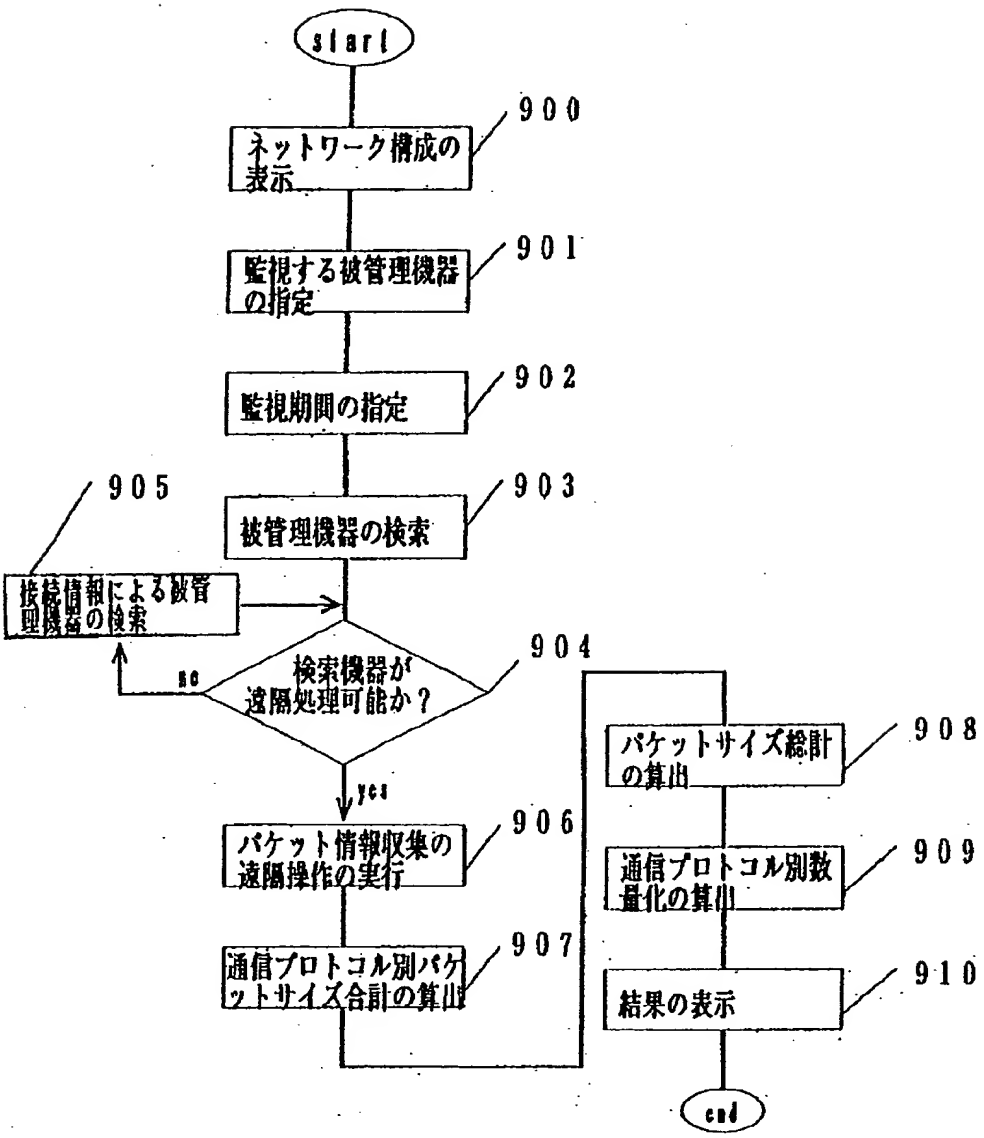
4300　4301　4302

ID	管理者 名	所属
101	佐藤 花子	設計
102	田中 次郎	企画
⋮	⋮	⋮

430

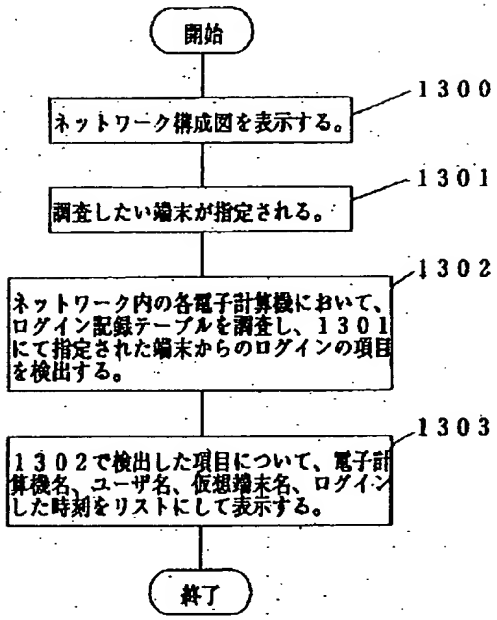
【図９】

図９


start
900
ネットワーク構成の表示
901
監視する被管理機器の指定
902
監視期間の指定
905
接続情報による被管理機器の検索
903
被管理機器の検索
904
検索機器が遠隔処理可能か？
no
yes
906
パケット情報収集の遠隔操作の実行
907
通信プロトコル別パケットサイズ合計の算出
908
パケットサイズ総計の算出
909
通信プロトコル別数量化の算出
910
結果の表示
end

【図１３】

図１３



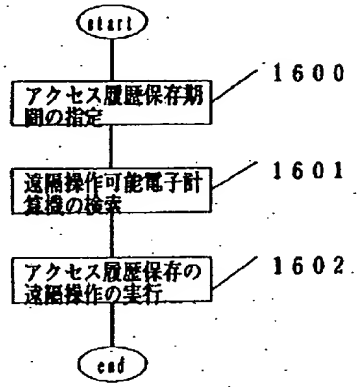
【図１５】

図１５

1500 電子計算機名	1501 ユーザ名	1502 仮想端末名	1502 ログインした時刻
電子計算機１	USER2	tty3	92.11.1. 10:10:00
電子計算機２	root	tty1	92.11.1. 10:20:30
：	：	：	：

【図１６】

図１６



【図１４】

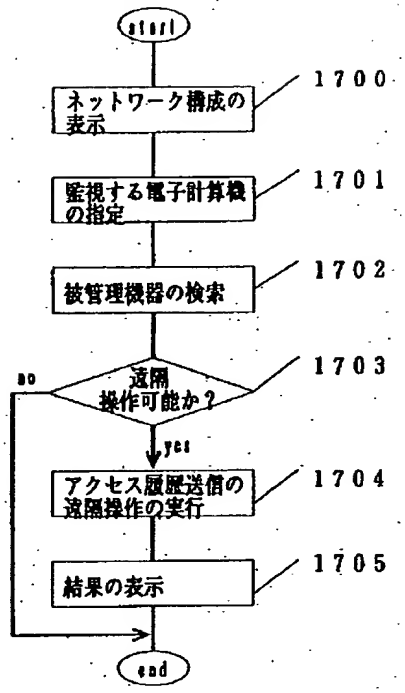
図１４

1400 ログインしたユーザ名	1401 使用した仮想端末名	1402 ログインした端末名	1403 ログインした時刻	1404 ログアウトした時刻	1405 ログインする前のユーザ名
USER2	tty3	端末１	92.11.1. 10:10:00		
USER3	tty2	端末２	92.11.1. 10:15:05	92.11.1. 12:10:00	USER6
root	tty1	端末１	92.11.1. 10:20:30	92.11.1. 10:40:30	USER2
user1	tty7	端末３	92.11.1. 10:23:10	92.11.1. 12:40:43	
root	tty4	端末４	92.11.1. 10:29:00	92.11.1. 11:00:00	
：	：	：	：	：	：

140

【図１７】

図１７



【図１８】

図１８

1800 アクセスユーザ	1801 アクセス方法	1802 アクセス日時
aak	read	92/05/30
mariko	write	92/06/01
yumiko	write	92/08/16
⋮	⋮	⋮

180

【図１９】

図１９

ファイル名	アクセスユーザ	アクセス方法	アクセス日時
/etc/passwd	aak	read	92/05/30
/etc/group	mariko	write	92/06/01
/etc/hosts	yumiko	write	92/08/16
	⋮	⋮	⋮

【図２２】

図２２

2200 プログラム名	2201 ユーザ名	2202 起動した仮想端末名	2203 起動した端末名	2204 起動時刻
user2	prog1	tty3	端末1	92.11.1. 10:15:30
user1	prog1	tty7	端末3	92.11.1. 10:24:00
root	prog3	tty4	端末4	92.11.1. 10:29:15
⋮	⋮	⋮	⋮	⋮

【図３２】

図３２

3200 プログラム名	3201 プログラムの所有者	3202 起動可能なユーザ	3203 稼働時のモード
prog1	root	全ユーザ	特権
prog2	user1	user1	一般
prog3	root	root	特権
⋮	⋮	⋮	⋮

320

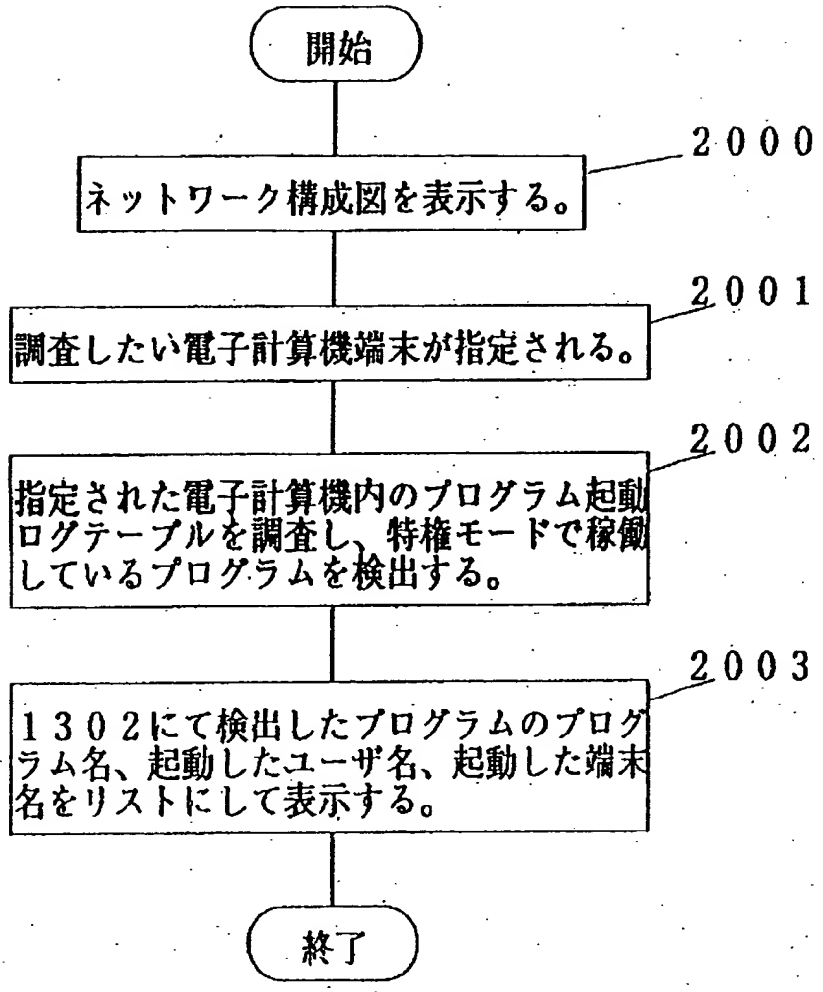
【図３４】

図３４

3400 プログラム名	3401 プログラムの所有者	3402 起動可能なユーザ
prog1	root	全ユーザ
⋮	⋮	⋮

【図２０】

図２０



【図２４】

図２４

2400 仮想端末名	2401 端末名	2402 ログインしていた時間帯	2403 特権ユーザにログインしたユーザ名
ｔｔｙ１	端末１	92.11.1. 10:20:30 ～ 92.11.1 10:40:30	ｕｓｅｒ２
ｔｔｙ４	端末４	92.11.1. 10:29:00 ～ 92.11.1. 10:50:00	
：	：	：	：

240

【図２１】

図２１

2100 起動したユーザ名	2101 起動したプログラム名	2102 起動した仮想端末名	2103 起動した端末名	2104 起動時刻	2105 終了時刻	2106 起動時のモード
user2	prog10	tty3	端末1	92.11.1. 10:11:00	92.11.1. 10:11:30	一般
user2	prog1	tty3	端末1	92.11.1. 10:14:30		特権
user3	prog15	tty2	端末2	92.11.1. 10:16:30		一般
user1	prog1	tty7	端末3	92.11.1. 10:24:00		特権
root	prog1	tty1	端末1	92.11.1. 10:25:00	92.11.1. 10:26:00	特権
root	prog3	tty4	端末4	92.11.1. 10:29:15		特権
⋮	⋮	⋮	⋮	⋮	⋮	⋮

210

【図３６】

図３６

3600 電子計算機名	3601 監視プログラム名	3602 重要度
電子計算機1	login-check	大
電子計算機1	police	小
電子計算機1	program-check	大
電子計算機2	login-check	大
⋮	⋮	⋮

360

【図２５】

図２５

2500 仮想端末名	2501 ログインした端末名	2502 起動したプログラム名	2503 起動時刻	2504 終了時刻	2505 ログインをしたユーザ名
tty1	端末1	prog1	92.11.1. 10:25:00	92.11.1. 10:26:00	user2
tty4	端末4	prog3	92.11.1. 10:29:15		
⋮	⋮	⋮	⋮	⋮	⋮

【図２７】

図２７

2700 ファイル名	2701 ユーザアクセス	2702 グループアクセス	2703 その他アクセス	2704 所有者	2705 所有者のグループ
/etc/passwd	110	100	100	root	system
/etc/group	110	100	100	root	system
/etc/hosts	110	100	100	root	system
⋮	⋮	⋮	⋮	⋮	⋮

270

【図４２】

図４２

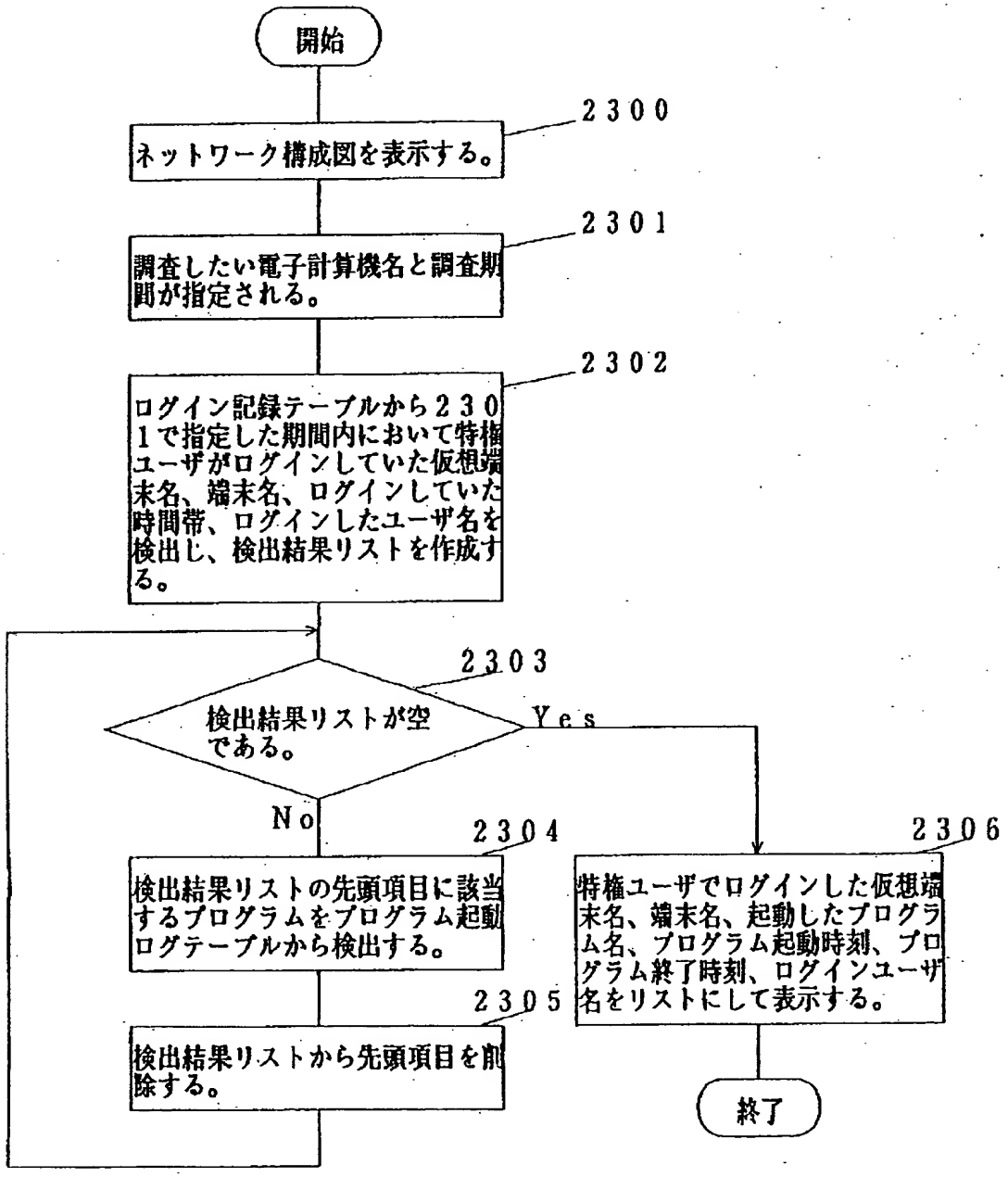
4200 YES／NO処理テーブル 4201

処理番号	処理内容
100	管理者にセキュリティホールの内容をメール送信
200	該当プロセスを消去
300	該当アカウントのユーザに警告メールを送信
⋮	⋮

420

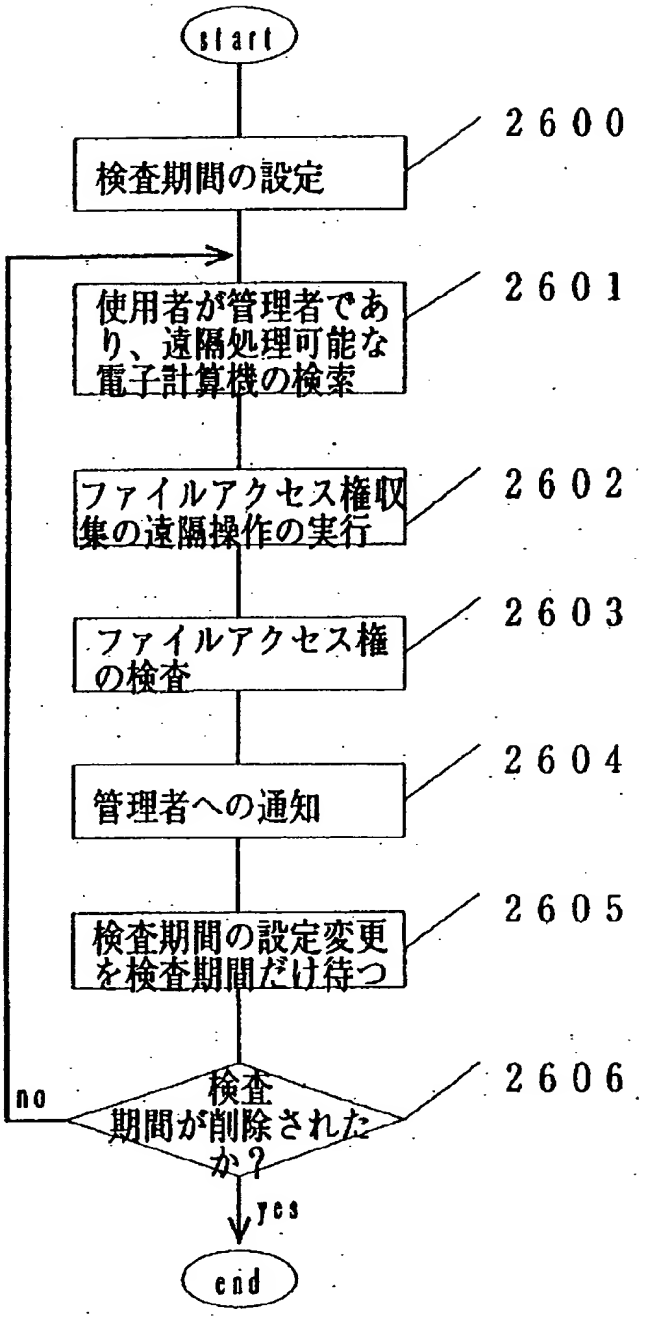
【図２３】

図２３


開始
2300
ネットワーク構成図を表示する。
2301
調査したい電子計算機名と調査期間が指定される。
2302
ログイン記録テーブルから２３０１で指定した期間内において特権ユーザがログインしていた仮想端末名、端末名、ログインしていた時間帯、ログインしたユーザ名を検出し、検出結果リストを作成する。
2303
検出結果リストが空である。
Yes
No
2304
検出結果リストの先頭項目に該当するプログラムをプログラム起動ログテーブルから検出する。
2305
検出結果リストから先頭項目を削除する。
2306
特権ユーザでログインした仮想端末名、端末名、起動したプログラム名、プログラム起動時刻、プログラム終了時刻、ログインユーザ名をリストにして表示する。
終了

【図２６】

図２６



【図３３】

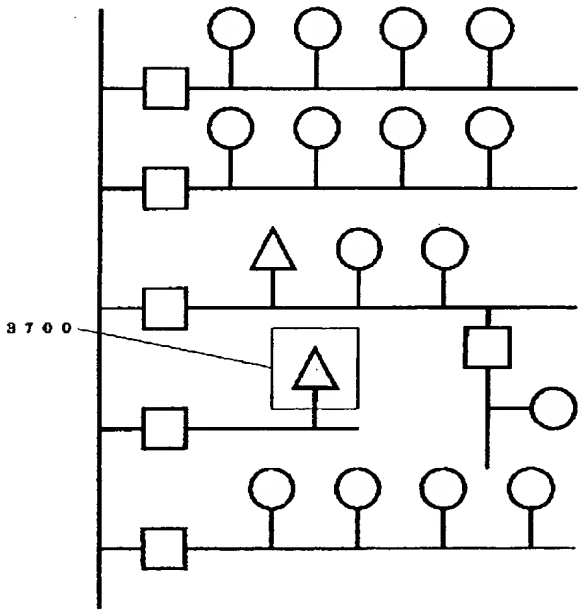
図３３

プログラム名	プログラムの所有者	起動可能なユーザ	稼働時のモード
prog1	root	root	特権
prog1	root	root	特権
⋮	⋮	⋮	⋮

330

【図３７】

図３７



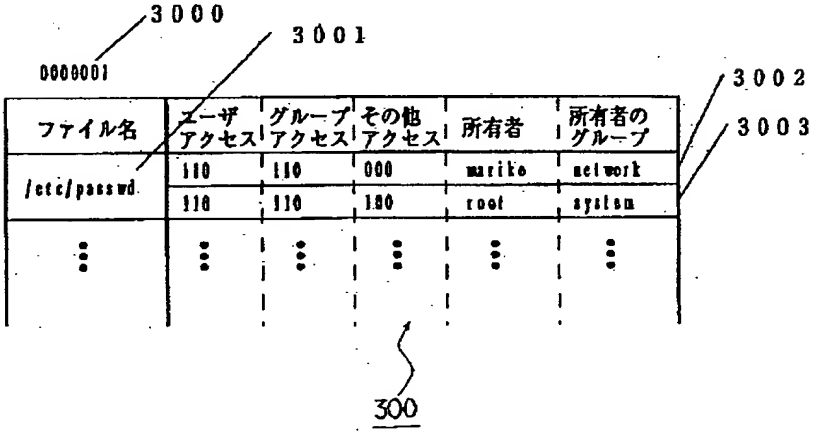
【図２９】

図２９

ファイル名	ユーザアクセス	グループアクセス	その他アクセス	所有者	所有者のグループ
/etc/passwd	110	110	000	mariko	network
/etc/group	110	100	000	nak	DB
/etc/hosts	110	000	100	root	system
⋮	⋮	⋮	⋮	⋮	⋮

【図３０】

図３０



【図４１】

図４１

セキュリティ対策テーブル

4100 セキュリティ対策ID	4101 チェック内容	4102 YES処理	4103 NO処理
A	プロセスが稼働中である	200	300
B	ユーザは管理者である	400	100
C	外部ユーザが認可されている	E	D
⋮	⋮	⋮	⋮

410

【図４４】

図４４

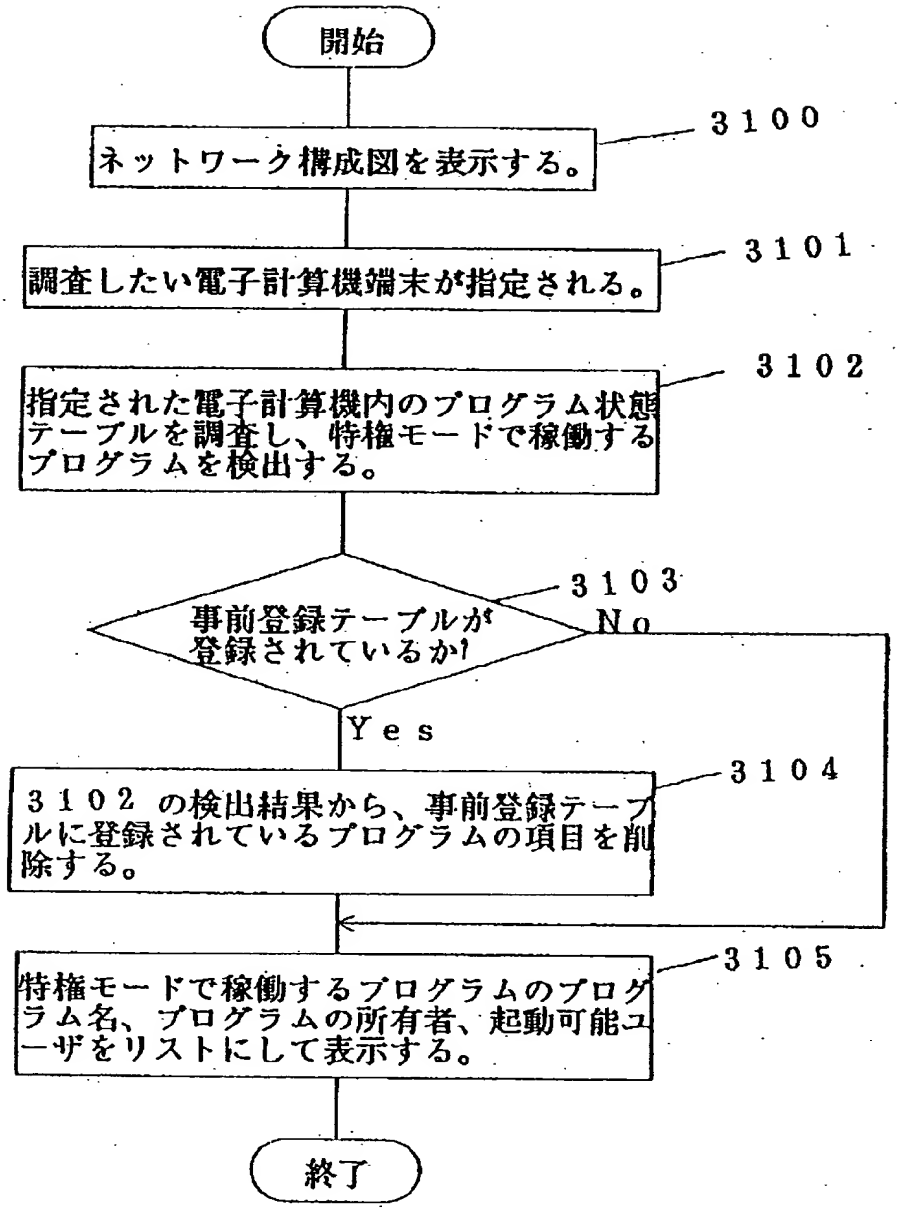
外部ユーザテーブル

4400 ID	4401 外部ネットワーク	4402 ユーザ名	4403 所属
1000	A大学	鈴木教授	理学部
1001	B電気会社	斉藤部長	システム部
⋮	⋮	⋮	⋮

440

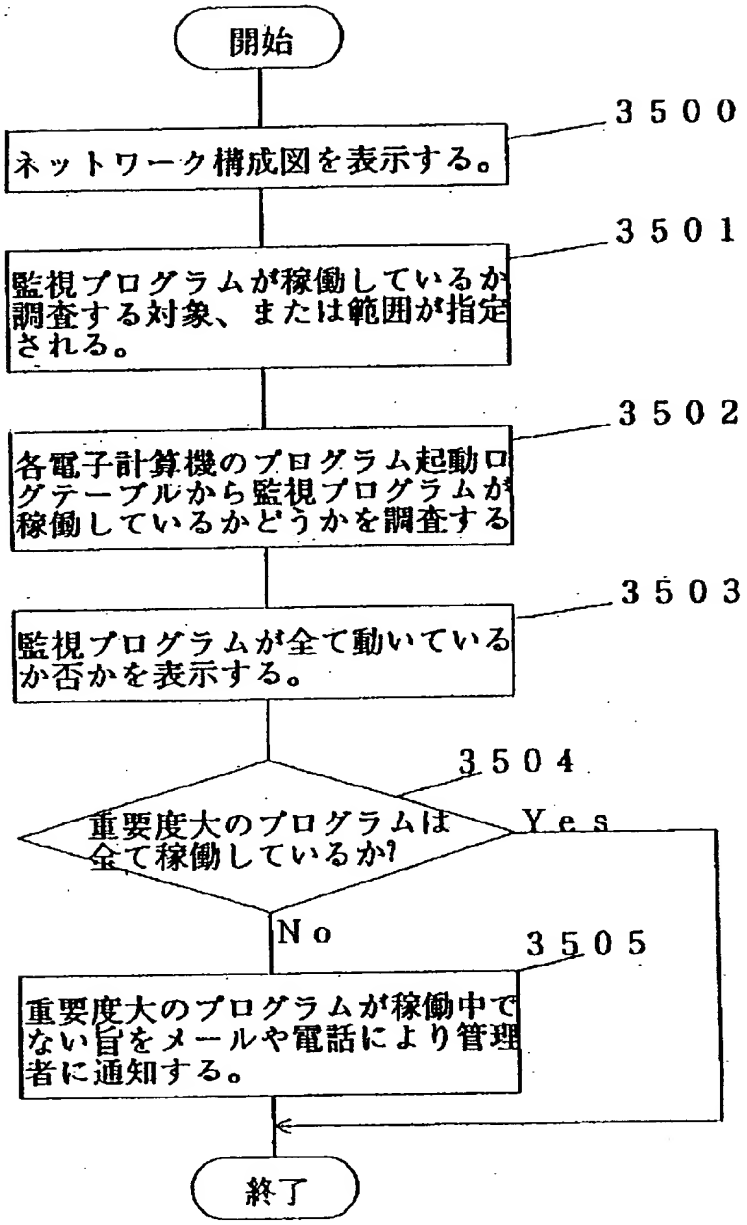
【図３１】

図３１


開始
ネットワーク構成図を表示する。
3100
調査したい電子計算機端末が指定される。
3101
指定された電子計算機内のプログラム状態テーブルを調査し、特権モードで稼働するプログラムを検出する。
3102
事前登録テーブルが登録されているか?
3103
No
Yes
３１０２の検出結果から、事前登録テーブルに登録されているプログラムの項目を削除する。
3104
特権モードで稼働するプログラムのプログラム名、プログラムの所有者、起動可能ユーザをリストにして表示する。
3105
終了

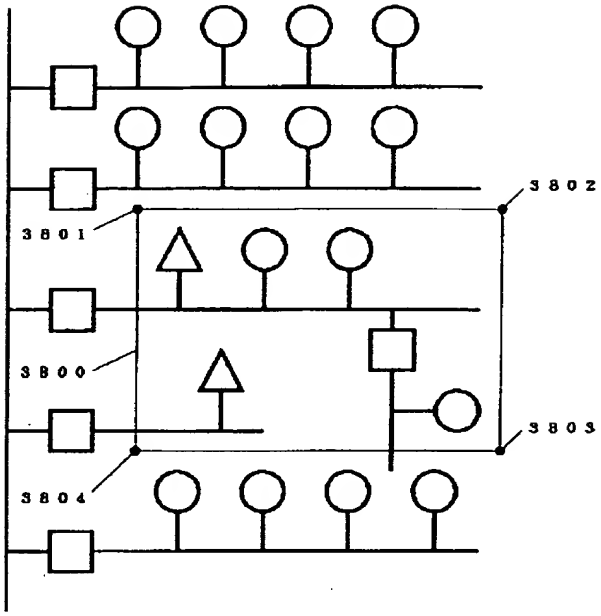
【図３５】

図３５


開始
３５００
ネットワーク構成図を表示する。
３５０１
監視プログラムが稼働しているか調査する対象、または範囲が指定される。
３５０２
各電子計算機のプログラム起動ログテーブルから監視プログラムが稼働しているかどうかを調査する
３５０３
監視プログラムが全て動いているか否かを表示する。
３５０４
重要度大のプログラムは全て稼働しているか?
Ｙｅｓ
Ｎｏ
３５０５
重要度大のプログラムが稼働中でない旨をメールや電話により管理者に通知する。
終了

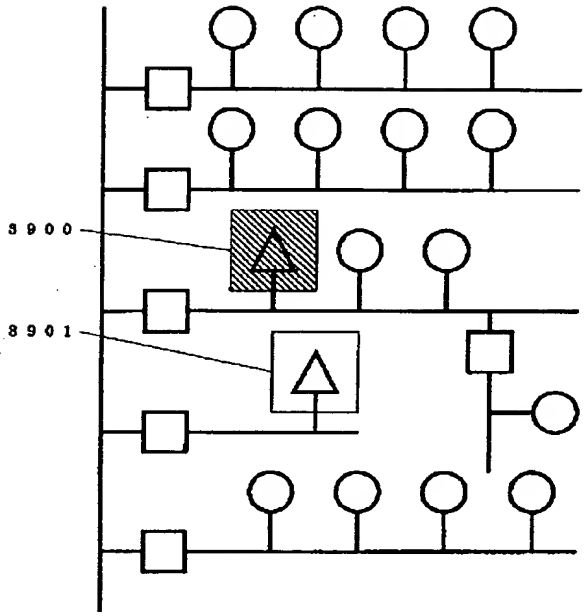
【図３８】

図３８



【図３９】

図３９



【図４０】

図４０

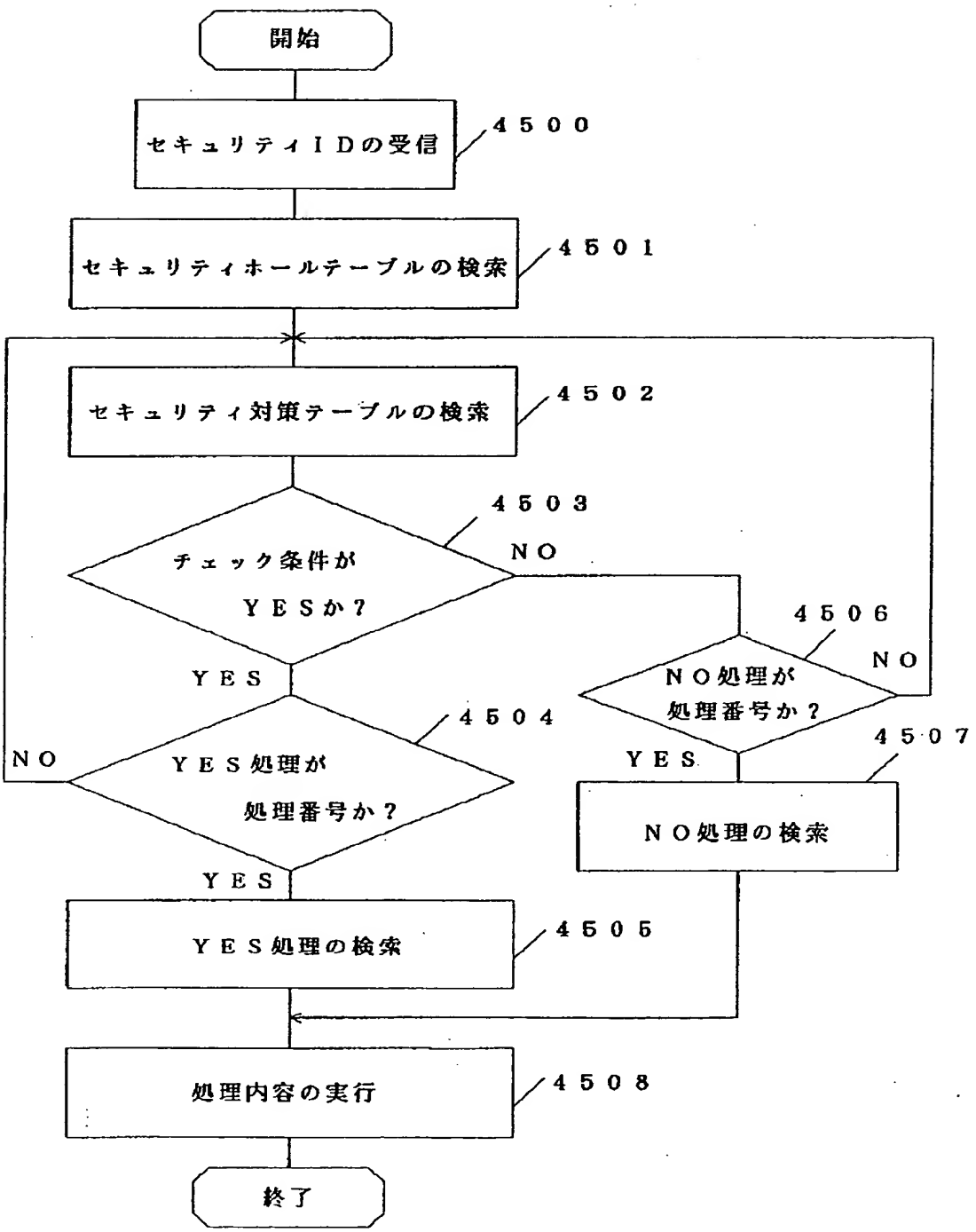
セキュリティホールテーブル

4000 セキュリティＩＤ	4001 セキュリティホールの内容	4002 セキュリティ対策ＩＤ
1	不正アカウントのユーザ	A
2	不正な特権モードプロセスあり	B
3	外部ネットワークからのログイン試行あり	C
・	・	・

400

【図４５】

図４５


開始
セキュリティＩＤの受信
４５００
セキュリティホールテーブルの検索
４５０１
セキュリティ対策テーブルの検索
４５０２
４５０３
チェック条件が
ＹＥＳか？
ＮＯ
ＹＥＳ
４５０６
ＮＯ処理が
処理番号か？
ＮＯ
４５０４
ＮＯ
ＹＥＳ処理が
処理番号か？
ＹＥＳ
４５０７
ＹＥＳ
ＮＯ処理の検索
ＹＥＳ処理の検索
４５０５
処理内容の実行
４５０８
終了

フロントページの続き

(51) Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
12/26				
H04M 3/42		E		
		8732-5K	H04L 11/08	

(72)発明者　堤　俊之
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会
社内